MAANPUOLUSTUSKORKEAKOULU

BYOD-LAITTEIDEN TIETOTURVA

Pro Gradu -tutkielma

Yliluutnantti
Lauri Maskulin

Sotatieteiden maisterikurssi 7
Merisotalinja

Huhtikuu 2018

MAANPUOLUSTUSKORKEAKOULU

Kurssi **Sotatieteiden maisterikurssi 7**	Linja **Merisotalinja**
Tekijä **Yliluutnantti Lauri Maskulin**	
Tutkielman nimi **BYOD-LAITTEIDEN TIETOTURVA**	
Oppiaine johon työ liittyy Sotatekniikka	Säilytyspaikka MPKK:n kurssikirjasto
Aika Huhtikuu 2018	Tekstisivuja 63 Liitesivuja 1

TIIVISTELMÄ

Bring Your Own Device eli BYOD on toimintatapa, jossa organisaatio sallii työntekijän itsekustantamansa päätelaiteen käytön jokapäiväisessä työnteossa. Tutkimusten mukaan työntekijöiden motivaatio ja tehokkuus kasvavat oman päätelaitteen työkäytön sallimisen myötä. Itsekustannetulla päätelaitteella eli BYOD-laitteella on työn tehokkuuden lisäämisen ohella myös varjopuolensa. Tutkimuksen tavoitteena on selvittää BYOD-laitteiden tietoturvallisuus ja niiden keskeisimmät tietoturvariskit organisaatiolle. Tutkimus rajataan käsittelemään älypuhelimien, tablettien ja kannettavien tietokoneiden BYOD-käyttöä normaaliolojen organisaatioissa. Tutkimusmenetelminä käytetään kirjallisuusanalyysia ja teemahaastattelua. Kirjallisuusanalyysin aineistona käytetään tietoturvakirjallisuutta, tutkimuksia, artikkeleita ja internet-lähteitä. Tutkimuksessa käsitellään organisaation tietoturvallisuuden luomista ja ylläpitoa, Bring Your Own Device-käsitteen kokonaisuutta sekä yleisimpien käyttöjärjestelmien tietoturvahaavoittuvuuksia. Tutkimukseen haastateltiin viittä puolustusvoimien ja neljää kyberturvayhtiö Nixu Oyj:n työntekijää. Haastateltavilla on vuosien kokemus tietoturvatyöstä sen eri tehtävissä.

Tutkimuksen tuloksena BYOD-laite on potentiaalinen tietoturvariski organisaatiolle. Riskien minimointi on mahdollista oikealla tietoturvapolitiikalla ja BYOD-ohjeistuksella sekä käytettävien ohjelmien avulla. Erityisesti päivitystuen ulkopuolelle jäävä päätelaite sisältää tietoturvahaavoittuvuuksia. Haittaohjelman saastuttama BYOD-laite avaa oven hyökkäyksille liittyessään organisaation verkkoon. Suurin uhka on tiedon vuotaminen BYOD-laitteen kautta organisaation ulkopuolelle. BYOD-laitteiden hallinta on turvallisuuden luomisessa tärkeää. Hallinnan avulla organisaation verkkoon ei päästetä päätelaitteita, jotka eivät täytä verkolle asetettuja tietoturvavaatimuksia, kuten ajantasaisia päivityksiä.

AVAINSANAT

Bring Your Own Device, BYOD, BYOD-laite, tietoturva

BYOD-LAITTEIDEN TIETOTURVA

KUVAT JA TAULUKOT

BYOD-LAITTEIDEN TIETOTURVA

1. JOHDANTO

Henkilökohtaisten päätelaitteiden määrä kotitalouksissa on lisääntynyt viimeisen vuosikymmenen aikana räjähdysmäisesti. Käännekohtana henkilökohtaisten laitteiden lisääntymiseen voidaan pitää vuoden 2010 loppua, jolloin Apple julkaisi ensimmäisen version iPad-tablet-tietokoneestaan. Yhdysvalloissa iPadin julkaisun myötä tuhannet opiskelijat ja työntekijät toivat uudet tabletit mukanaan työpisteilleen.[1] Cisco VNI Forecastin mukaan vuoteen 2021 mennessä maailmassa arvioidaan olevan 11,6 miljardia internetyhteyttä käyttävää mobiililaitetta. Tämä tarkoittaa puolitoista päätelaitetta jokaista maailman ihmistä kohden.[2] Verrattuna muihin maanosiin Pohjois-Amerikassa ja Euroopassa älylaitteita on vieläkin enemmän ihmistä kohti. Älypuhelimet, tabletit sekä kannettavat tietokoneet kulkevat päivittäin mukanamme kotona, kaupungilla sekä työpaikalla. Henkilökohtaiset päätelaitteemme ovat synkronoituja omiin sähköposti-palvelimiin sekä sosiaaliseen mediaan. Yhteys internetin kautta ympäröivään maailmaan on tätä päivää.[3]

Itsekustannetut mobiililaitteet liikkuvat työntekijöiden mukana työpaikoille ja organisaation salliessa niiden käytön työnteossa, puhutaan BYOD-toimintatavasta. BYOD on lyhenne englannin kielen sanoista Bring Your Own Device, joka tarkoittaa karkeasti suomennettuna *Tuo Oma Laitteesi*. Muita käytettäviä termejä ilmiölle on muun muassa BYOT – Bring Your Own Technology, *Tuo Oma Teknologiasi*. [4]s.35 BYOD-toimintatapa on osa organisaation tietoturvapolitiikkaa ja ilmiönä organisaation hyväksymä. Henkilökohtaisen päätelaitteen käyttäminen työpaikalla ei suoranaisesti ole BYOD-käyttöä ellei sillä käsitellä työnteon vaatimia järjestelmiä ja tietoa. Työntekijöiden elektroniikan käyttö organisaatioissa luo suuria haasteita sekä mahdollisuuksia.[5][6] BYOD on tapa työn tekemiseen, eikä niinkään tekniikkaa. Toimintatavassa organisaation työntekijä tuo itsekustantamansa teknologisen laitteen mukanaan työpaikalle tai etätyöpisteelle ja käyttää sitä tai sen sovelluksia työntekoon. BYOD-termi sisältää kaikenlaiset päätelaitteet, ulkoiset kovalevyt ja muistitikut sekä kamerat, joita työnteossa voidaan hyödyntää. BYOD:in sallivan organisaation työntekijä liittyy organisaation tieto-

verkkoon ja kykenee suorittamaan päivittäisiä työtehtäviään omalla laitteella, organisaation tietoverkossa.[4] IBM:n tekemän tutkimuksen mukaan vuoteen 2016 mennessä suurin osa Yhdysvalloissa toimivista suurista yrityksistä sallii työntekijöidensä käyttää älypuhelinta tai tablettia työssään.[7] s.2

Työntekijät tuntevat omat päätelaitteensa ja sen ominaisuudet - kuten älypuhelimen tai kannettavan tietokoneen – muun muassa tästä syystä ne koetaan usein helppokäyttöisemmiksi kuin työnantajan tarjoamat päätelaitteet. Henkilökohtainen päätelaite mahdollistaa joustavamman työnteon liikkuvuutensa ansiosta. Oma laite on aina mukana. Accenturen tekemässä globaalissa tutkimuksessa jopa puolet työntekijöistä kokee henkilökohtaiset päätelaitteet sovelluksineen työpaikan tarjoamia laitteita ja sovelluksia hyödyllisemmiksi.[5] Consumerization of Enterprise IT -tutkimuksessa haastateltiin yli 4000 työntekijää sekä yli 300 yritys- ja tietohallintojohtajaa 16 maasta ja viideltä mantereelta Accenture Institute for High Performance – tutkimusyksikön toimesta. Tutkimukseen haastateltavista työntekijöistä neljännes käyttää omia päätelaitteitaan ja sovelluksiaan päivittäisissä työtehtävissään.[5] BYOD-toimintatapa on suosittua työntekijöiden keskuudessa, koska työntekoon halutaan käyttää vain yhtä päätelaitetta useamman sijaan. Looginen vaihtoehto on oma älypuhelin, tabletti tai kannettava tietokone, koska niiden käyttö on tuttua ja ne ovat käden ulottuvilla jatkuvasti.[8] s.66–68

Henkilökohtaisten päätelaitteiden määrän kasvaessa niiden BYOD-käytön voidaan odottaa kasvavan organisaatioissa, näin saattaa käydä myös puolustusvoimissa. BYOD-käytön lisääntyminen tuo mukanaan organisaatiolle työnteon joustavuuden ohella käytännön haasteita sekä tietoturvariskejä. Henkilökohtaisten laitteiden käytön haasteisiin on varauduttava organisaation IT-infrastruktuurin ja henkilökunnan ohjeistuksen osalta. Ajankohtaisuus ja ilmiön yleistyminen myös omassa organisaatiossa herätti mielenkiinnon tutkittavaa aihetta kohtaan. Pidän realistisena vaihtoehtona, että lähitulevaisuudessa suorittaisin joitain työtehtäviäni kollegoiden tavoin omalla päätelaitteella, esimerkiksi älypuhelimella tai tabletilla. Perehtyessäni BYOD-käsitteeseen, lähteissä korostuu koko organisaation vastuu tietoturvallisuudessa. Vastuu ei ole yksin työntekijällä, joka käyttää omaa laitettaan työntekoon, vaan koko organisaatiolla ja ensisijaisesti organisaation johdolla, jonka on ymmärrettävä BYOD jokapäiväisenä, tärkeänä osana organisaation toimintaa.

Puolustusvoimien johtamisen tuen teknisten ratkaisujen kehittämiselle on olemassa merkittävä tarve. Muuhun yhteiskuntaan integroituneet puolustusvoimat tarvitsevat toimivat yhteydet kommunikaatioon muiden viranomaisten ja yhteistoimintatahojen kanssa. Yhteistoiminnan varmistamiseksi olemassa olevien järjestelmien suorituskyky on saatava laajemmin puolustusvoimien käyttöön. Johtamisen tuen konsepti 2030:n mukaan puolustusvoimien tulisi hyödyntää paremmin olemassa olevia teknologioita.[9]s.5 On siis odotettavissa, että BYOD-toimintatapaa tullaan hyödyntämään enemmän tulevaisuuden maanpuolustuksessa.

1.1. Tutkimuksen tavoitteet ja tutkimuskysymykset

Tutkimuksen tavoitteena on selvittää BYOD-laitteen eli työvälineenä käytettävän työntekijän itsekustantaman päätelaitteen organisaatioon kohdistamat tietoturvariskit. Valtionhallinnon tietoturvasanastossa tietoturvariski määritellään tietoon, tietoliikenteeseen tai tietojärjestelmään kohdistuvana vahingon vaarana.[10]s.111 Tutkimuksessa käsitellään organisaation tietoturvallisuuden luomista ja ylläpitoa, Bring Your Own Device-käsitettä sekä yleisimpien käyttöjärjestelmien tietoturvahaavoittuvuuksia. BYOD-käsite on avattava perusteellisesti toimintatavan ymmärtämiseksi, jotta tutkimuksen pääkysymykseen on riittävät edellytykset vastata. Teemahaastatteluiden tukemana muodostetaan tutkimuksen johtopäätökset. Johtopäätöksissä vastataan tutkimuskysymyksiin ja pyritään esittelemään tietoturvallisin vaihtoehto organisaation BYOD-ympäristössä.

Tutkimuksen pääkysymyksenä on:

- *Millainen tietoturvariski BYOD-laite on organisaatiolle?*

Tutkimuksen pääkysymyksen tueksi on muodostettu kolme alakysymystä:

1. *Millaisia tietoturvauhkia kohdistuu organisaatioihin?*

2. *Miten BYOD-laitteiden käyttöjärjestelmät poikkeavat tietoturvaltaan?*

3. *Minkälaisia tietoturvavaatimuksia on BYOD-laitteen sovelluksilla?*

1.2. Tutkimuksen rajaus

Tutkielman tavoitteeseen peilaten työn keskiössä on BYOD-laite eli työntekijän henkilökohtaisesti kustantama päätelaite. Tässä tutkimuksessa BYOD-laitteella tarkoitetaan internetyhteydessä olevia älypuhelimia, tabletteja sekä kannettavia tietokoneita, joita käytetään normaalioloissa tavallisten työtehtävien suorittamiseen verkkoyhteyden välityksellä. BYOD-laitteella työntekijä on verkon kautta yhteydessä organisaation järjestelmään ja sillä käsitellään organisaation tiedostoja ja tietokantoja. Käsiteltäessä BYOD-laitetta rajataan ulkoiset kovalevyt, muistitikut, kamerat sekä muut tekniset laitteet tarkastelun ulkopuolelle. Laitevalmistajien kirjo on markkinoilla valtava, eikä tutkielman lopputuloksen kannalta nähdä tarpeelliseksi paneutua niin sanotulle rautatasolle eli laitevalmistajien päätelaitteiden eroavaisuuksiin. Älypuhelimia, tabletteja ja kannettavia tietokoneita käsitellään yleisellä tasolla eli millaiset tekniset ominaisuudet ovat tyypillisiä kyseisissä päätelaitetyypissä. Tutkimuksessa vertaillaan BYOD-laitteiden yleisimpien käyttöjärjestelmien tietoturvallisuutta niistä raportoitujen haavoittuvuuksien näkökulmasta. Vertailtavia käyttöjärjestelmiä ovat mobiililaitteilla käytettävät Android ja iOS sekä kannettavien tietokoneiden osalta Windows, Mac OS ja Linux.

Tietoturvan osalta käsitellään organisaation toimenpiteitä, vaatimuksia ja käytäntöjä BYOD-toimintatavan mahdollistamiseksi, sen käyttämissä sovelluksissa sekä työntekijöiden henkilökohtaisissa BYOD-laitteissa. Tutkielmassa organisaatiota käsitellään yleisluonteisena käsitteenä. Voidaan todeta, että organisaatioissa on oman toiminnan kannalta salassa pidettävää tietoa, jonka ei haluta päätyvän ulkopuolisten käsiin. Organisaatioiden suorittamat tietoturvatoimenpiteet noudattavat pääasiallisesti samoja suuntaviivoja ja tämän perusteella organisaatiota voidaan käsitellä geneerisenä käsitteenä.

Turvaluokitukseltaan tutkielma on julkinen ja siinä käytettävä lähdemateriaali on peräisin julkisista lähteistä, kuten kirjallisuudesta, artikkeleista ja internetistä. Lähteenä ei ole käytetty turvaluokiteltua materiaalia. Tutkimuksen julkisuuden vuoksi tiettyyn organisaatioon kohdistuvia yksityiskohtia ei käsitellä vaan näkökulma pidetään yleisellä tasolla.

1.3. Tutkimusmenetelmät

Tutkielma on kvalitatiivinen eli laadullinen tutkimus. Kvalitatiivisessa tutkimuksessa lähtökohtana on ilmiön kokonaisvaltainen tutkiminen ja sen ymmärtäminen.[11] Käytettävinä tutkimusmenetelminä ovat kirjallisuusanalyysi sekä teemahaastattelu. Kvalitatiivinen tutkimustapa on valintana perusteltu, koska Bring Your Own Device-käytäntö on yleistynyt vasta viimeisen vuosikymmenen aikana eikä aihetta ole vielä tutkittu laajasti.[11]

Kirjallisuusanalyysillä saadaan tutkielmalle vankka teoriapohja ja keskeiset käsitteet kyetään määrittelemään tarkasti. Kirjallisuusanalyysillä kirjallisuus-, artikkeli-, tutkimus- sekä internet-lähteistä kootusta tiedosta saadaan määriteltyä BYOD-toimintatapa teknisine toteutuksineen sekä käsitteineen. Käyttöjärjestelmien tietoturvavertailu suoritetaan analysoimalla niistä raportoituja haavoittuvuuksia sekä julkaistuja koventamisohjeita. Vertailun tueksi käyttöjärjestelmistä kerrotaan keskeisiä turvallisuuteen vaikuttavia kokonaisuuksia ja tunnettuja haavoittuvuuksia. Kirjallisuusanalyysillä kyetään tuottamaan perusteet tutkimuksen teemahaastattelujen pohjaksi sekä haastattelussa käytettävien aihepiirien ja kysymysten laadintaan. Teoriapohjan ollessa kattava, ei teemahaastatteluiden jälkeen ole tarvetta avata tutkimuksen kannalta täysin uusia käsitteitä, jotka haastatteluiden vastausaineisto tuo tullessaan. Kirjallisuusanalyysillä pyritään saamaan vastauksia tutkimuksen kaikkiin apukysymyksiin.

Teemahaastattelu on haastattelulajina lomake- ja avoimen haastattelun välimuoto.[11] Kysymysten aihepiiri määritetään etukäteen ja haastattelu etenee tutkijan kontrollissa. Teemahaastatteluilla selvitetään tietoturvan parissa työskentelevien näkemyksiä Bring Your Own Device-toimintatavasta ja BYOD-laitteen tietoturvallisuudesta. Haastatteluiden avulla selvitetään, millaisilla toimintatavoilla päästään tietoturvastrategian määrittelemälle tasolle. Kvalitatiivisessa tutkimuksessa teemahaastattelu soveltuu tutkielman haastattelutyypiksi paremmin kuin lomakehaastattelu. Lomakkeiden kysymysasettelu saattaisi rajoittaa haastateltavien vastauksia selvitettäessä heidän henkilökohtaisia suhtautumisiaan sekä näkemyksiään BYOD-käytäntöihin, eivätkä näin heidän omat kokemukset pääsisi halutulla tavalla esille. Teemahaastatteluissa käsitellään kahdeksaa kysymystä, jottei se muutu strukturoiduksi haastatteluksi.[11]

Tutkimuksen teemahaastattelut toteutettiin alkuvuodesta 2018. Tutkimukseen haastateltiin tietoturva- sekä tietohallinto-osaajia Puolustusvoimien tutkimuslaitokselta, Pääesikunnasta, Maanpuolustuskorkeakoululta sekä kyberturvayhtiö Nixu Oyj:stä. Teemahaastatteluiden toteutuksesta, sisällöstä ja vastauksista enemmän 5. pääluvussa. Teemahaastattelulla pyritään saamaan vastauksia tutkimuksen apukysymyksiin.

1.4. Lähdemateriaali ja aiemmat tutkimukset

BYOD-toimintatapa on ilmiönä uusi ja yleistynyt merkittävästi viimeisen vuosikymmenen aikana älypuhelinten ja tablettien yleistymisen myötä. Aihepiiristä on kirjoitettu useita, pääasiassa englannin kielisiä artikkeleita ja oppaita. Näkökulma on pääsääntöisesti yritysmaailmassa ja BYOD-toimintatavan sallivien organisaatioiden hyödyissä sekä haasteissa. Yleistäen henkilökohtaisten laitteiden käyttö lisää työntekijöiden motivaatiota ja sitä kautta työtehoa sekä tuo mukanaan tietoturvariskejä. Positiivisten ja negatiivisten asioiden ohella käsitellään oikeanlaista tietoturvastrategiaa, jolla organisaatio saa yleistyvästä ilmiöstä tietoturvallisesti suurimman mahdollisen hyödyn.

Bring Your Own Device-toimintavasta on tehty akateemisia tutkimuksia. Yleistäen tutkimusten fokus on yritysmaailmassa eli minkälaisia uhkia ja mahdollisuuksia omien päätelaitteiden käyttö tuo, sekä miten yritys saa hyödynnettyä trendin, maksimoidakseen tehokkuuden ja voiton, tietoturvaa unohtamatta. Suuret tietoliikenne- ja tietoturvayritykset ovat omissa tutkimuksissaan selvittäneet BYOD-toimintatavan yleistymistä sekä tietoturva-ongelmien, kuten virustartuntojen määriä. Tässä luvussa ei keskitytä niihin tarkemmin, vaan tutkielmassa palataan tuloksiin tarvittaessa myöhemmin.

Tämän tutkielman kannalta toinen keskeinen tutkimuskohde on käyttöjärjestelmät. Mobiililaitteiden käyttöjärjestelmiä on tutkittu ja vertailtu tietoturvan osalta korkeakoulujen lopputöissä sekä akateemisissa artikkeleissa. Käyttöjärjestelmien vertailun lähteinä käytetään CIS Benchmark kovennusohjeita, haavoittuvuustietoja sekä tietoturvatutkimuksia sekä käyttöjärjestelmistä julkaistuja tutkimuksia, raportteja ja oppaita. Tietoturvalähteinä käytetään tietoturvakirjallisuutta, -artikkeleita ja -ohjeita.

Turun Kauppakorkeakoulu on julkaissut vuonna 2012 Joonatan Voltin kirjoittaman pro gradu-tutkielman aiheesta *”Bring Your Own Device - trendin mahdollisuudet ja haasteet yrityksille”*. Tutkielmassa Voltti käsittelee, kuinka BYOD-trendin avulla yritys saisi tehostettua omia toimintatapojaan. Voltti haastatteli yhdeksää eri yritystä selvittäen näiden kokemuksia BYOD-käytöstä ja minkälaisia mahdollisuuksia trendi tuo yrityksen toimintaan.[12]

Lundin yliopiston kauppakorkeakoulu on julkaissut vuonna 2012 Fredrik Lunden ja Gustav Mattssonin kandidaatin tutkielman*”Bring Your Own Device - Risker och Möjligheter”*, joka käsittelee BYOD-toimintatavan riskejä ja mahdollisuuksia yrityksille.[13]

Sanna Eronen on tutkinut vuonna 2015 iOS:n, Androidin ja Windows Phonen mobiilikäyttöjärjestelmien tietoturvaominaisuuksia tietojenkäsittelyn koulutusohjelman opinnäytetyössään ”*Mobiilikäyttöjärjestelmien tietoturva”*. Mobiilikäyttöjärjestelmiä vertailemalla Eronen pyrki löytämään soveltuvimman mobiiliratkaisun julkishallinnon organisaatiolle.[14]

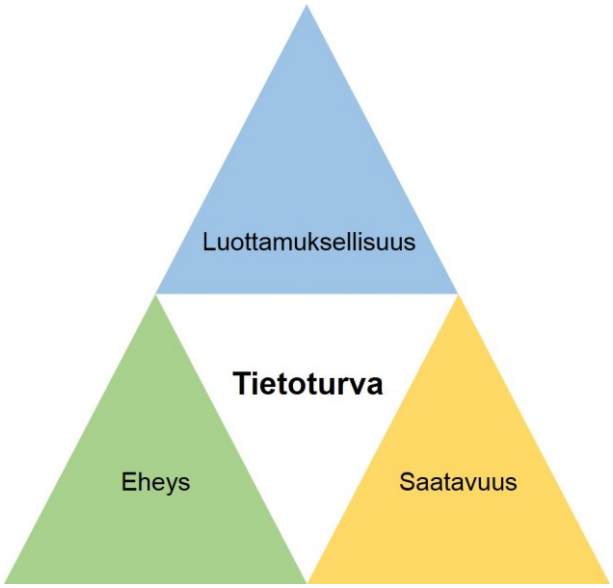
2. TIETOTURVA ORGANISAATIOSSA

2.1. Tietoturvallisuus

Tietoturvallisuus on osa organisaation kokonaisturvallisuutta.[15]s.27–28 Kaupallisten sekä voittoa tavoittelemattomien organisaatioiden toiminta perustuu tietoon ja sen hallintaan. Kaupallisella puolella fokus on voiton tavoittelussa, mutta kasvaneet uhat ovat pakottaneet organisaatiot huomioimaan tiedon suojaamisen ulkopuolisilta tahoilta aiempaa tehokkaammin. Andressin ja Winterfeldin mukaan organisaatiolle arkaluontoisen tiedon vuotamisella on taloudellisten menetysten lisäksi suurempiakin seurauksia.[16]s.194 Organisaation tietoturvan pettäessä salassa pidettävää tietoa päätyy organisaation sisällä henkilöille joiden käyttöoikeudet eivät riitä sen käsittelyyn tai kokonaan organisaation ulkopuolelle. Vuotanut tieto aiheuttaa sitä suuremman vahingon organisaatiolle, mitä salaisempaa se on, tai kuinka paljon tietoa päätyy vääriin käsiin. Tiedon vuotaessa organisaatiot saattavat menettää maineen lisäksi myös maksavia asiakkaita ja yhteistyökumppaneita. Vakavien tietoturvapuutteiden takia asiakkaat voivat kääntyä toisen palveluntarjoajan puoleen. Vuotaneen tiedon sisältöä voidaan muuttaa, eikä alkuperäisen, eheän tiedon sisällöstä voida enää varmistua. Alkuperäinen tieto voidaan palauttaa varmuuskopioista, mikäli ne eivät ole korruptoituneita. Pahimmassa tapauksessa tieto kerätään useista lähteistä, joka vie paljon taloudellisia resursseja. Vahingot ovat suoraan suhteessa häirityn palvelun kriittisyyteen.[17]s.40–43

Käsitteenä tietoturvallisuus on laaja ja monitasoinen ja sen määritelmät poikkeavat toisistaan joiltain osin. Perustana on ymmärrys siitä, että organisaation tärkein omaisuus on tieto sen kaikissa olomuodoissa.[16]s.194 Käsitteen määritelmiä yhdistää tiedon nopea saatavuus oikeassa muodossa henkilöille, joilla on siihen oikeus.[18] s.4-6 Klassisen määritelmän mukaan tietoturvallisuus on kolmen osatekijän summa. Tiedon luottamuksellisuus, eheys ja saatavuus muodostavat kolmestaan tietoturvallisuuden kokonaisuuden, johon organisaation tietojärjestelmien turvallisuuden suunnittelu perustuu.[19]s.22-24 Kuvassa 1 näytetään osatekijöiden muodostama kokonaisuus. Yksinkertaistettuna organisaation tietoturvallisuus on teknisten ja käytännön järjestelyiden kokonaisuus, joilla tiedon osatekijät suojataan ja tiedon arvo varmistetaan.[16]s.193-194 [19]s.21-24 Mikäli joku kolmesta periaatteesta pettää, on tietoturva vaarassa. Tästä syystä tietoturvallisuuden menetelmiä organisaatioissa on seurattava ja omia toimintatapoja kehitettävä jatkuvasti. Tietoturvallisuuden perustana olevien teknisten- ja käytännöntoimien avulla varmistetaan, ettei organisaation tietoa tai muuta omaisuutta päädy ulkopuolisille tahoille rikollisin menetelmin tai työntekijöiden toimesta. Tietoturvalla varmiste-

taan, että organisaatio kykenee jatkamaan normaalia jokapäiväistä toimintaansa.[17]s.31-32 [15]s.30



KUVA 1. Tiedon luottamuksellisuus(Confidentiality), eheys (Integrity) ja saatavuus (Availability) muodostavat tietoturvan kokonaisuuden. Mukaillen CIA-kolmiota [16]s.194

Luottamuksellisuus tarkoittaa, että tieto ei päädy ulkopuolisten käsiin organisaation sisällä tai sen ulkopuolella.[19]s.24 Tiedon päätyminen vääriin käsiin estetään sähköisellä kulunvalvonnalla ja – hallinnalla, käyttöoikeuksilla sekä suojeltavan tiedon salaamisella. Tiedon suojelemiseksi on huomioitava sen sijainti ja luonne. Käytetäänkö ja muokataanko sitä päätelaitteella vai onko se staattisena tallenteena verkkolevyllä tai pilvipalvelussa. Tiedon sijainti ja luonne vaikuttavat käytettäviin suojausmetodeihin.[16]s.194-195

Eheys tarkoittaa, että tietoa ei muuteta luvattomasti. Eheys saavutetaan estämällä luvattomat muutokset suojeltavassa tiedossa tai järjestelmän toiminnossa varmistamalla, että henkilöt, joilla ei ole siihen käyttöoikeuksia, eivät pääse muokkaamaan tiedon sisältöä. Tiedon eheys voidaan varmistaa seuraamalla alkuperäistiedostosta otettua sähköistä sormenjälkeä, jolla todennetaan tiedon aitous. Mikäli organisaatio ei ole selvillä tiedon sisällön luvattomista muutoksista, voivat seuraukset olla kohtalokkaita. Muuttunutta sisältöä käsitellään aitona ja alkuperäisenä, joten keskeiset organisaation tekemät päätökset saattavat pahimmassa tapauksessa perustua virheelliseen tietoon.[19]s.23 [16]s.195-196

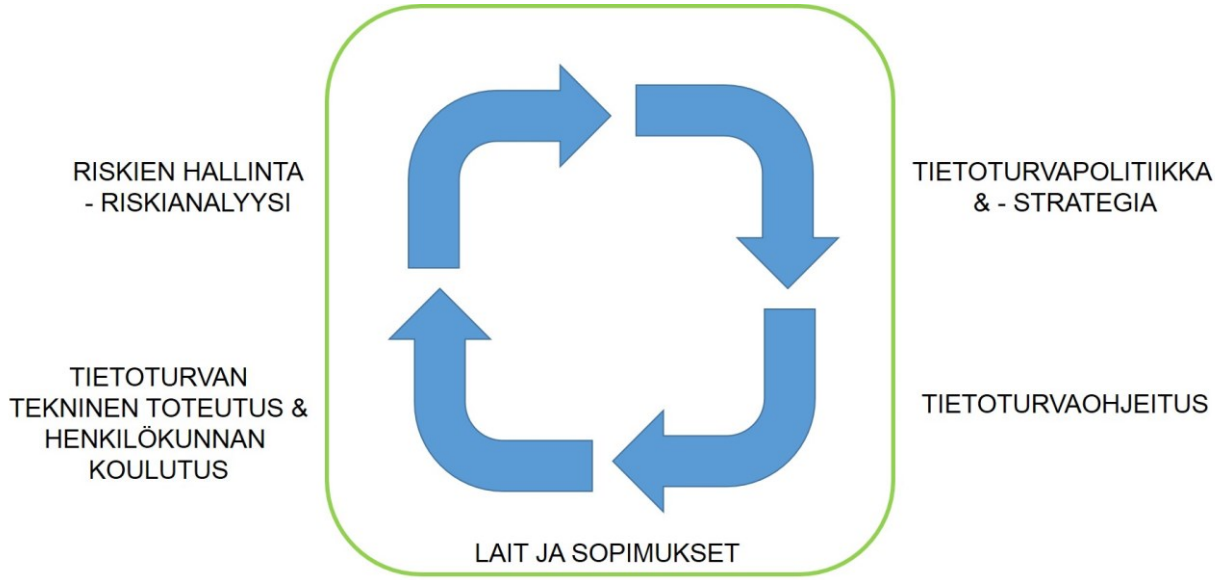
Saatavuus tarkoittaa, että käyttöoikeutettu henkilö pääsee halutessaan tietoon käsiksi. Tiedon jatkuva saatavuus on mahdollista organisaatioiden ollessa vastustuskykyisiä tallennettuun tietoon kohdistuvien hyökkäysten edessä. Hyökkäykset saattavat vahingoittaa tai poistaa organisaation tietoja tai estää sen pääsyn omistamaan tietoon. Tämä tarkoittaa myös sitä, että

organisaatioilla on oltava riittävän kestävä ympäristö järjestelmän häiriöiden selvittämiseksi. Tiedon käytettävyyteen vaikuttavia häiriöitä ovat esimerkiksi tietoliikenneongelmat ja puutteellinen sähkön saanti. Saatavuus saavutetaan tietoliikenneyhteyksien redundanttisuudella eli kahdentamisella sekä varmuuskopioinnilla. [19]s.23 [16]s.196

Tietoturvallisuuden perinteistä kolmijaollista käsitettä Hakala et al. täydentävät tiedon kiistättömyydellä (non-repudiation) ja pääsynvalvonnalla (access control). Määritelmän mukaan klassinen kolmijako ei huomioi riittävästi käytettäviä tietoteknisiä ratkaisuja, eikä tiedon omistajan ja tuottajan roolia.[18]s.5-6 Osatekijän kiistättömyydellä tarkoitetaan organisaation tietojärjestelmien suorittamaa seurantaa tietoa käsittelevistä henkilöistä. Seuranta tunnistaa ja dokumentoi tiedon käsittelijät järjestelmään. Tiedon kiistämättömyydellä varmistutaan sen alkuperästä ja mahdollisista luvattomista käyttötapauksista. Kiistättömyyteen pyritään oikeiden salausmenetelmien ja tunnistusmekanismien avulla.[18]s.5-6 Seurannan toteutus voidaan tehdä työntekijän henkilökohtaisella sirullisella toimikortilla tai vastaavalla ulkoisella tunnisteella, jota henkilön on käytettävä kirjautuessaan tai käyttäessään organisaation käytössä olevaa palvelua. Toimikortin rinnalla tunnistus voidaan toteuttaa myös biometrisesti, esimerkiksi sormenjälkitunnistimella.[18]s.124-125 Pääsynvalvonnalla rajoitetaan henkilöiden pääsyä tietoon, johon heidän oikeudet eivät riitä. Rajoitus toteutetaan esimerkiksi käyttöoikeuksien hallinnalla. [18] s.124–126

2.2. Tietoturvallisuuden jalkauttaminen

Tietoturva ja sen toteuttaminen ovat osa organisaation turvallisuutta ja sen hallintaa, sekä toiminnan suunnittelua ja johtamista.[19] s.21–22 Tietoturvallisuus vaatii organisaation johdolta oikean asennoitumisen sekä kaiken mahdollisen tuen. Riittävillä resursseilla johto varmistaa tietoturvallisuuden toteuttamisen, ylläpitämisen sekä jatkuvan kehittämisen. Tietoturvallisuus toimii, kun se toteutetaan ennakoivasti ja huomioidaan kaikissa organisaation päätöksissä. Riskien tiedostaminen ja niihin varautuminen mahdollistaa myös poikkeavien menettelyiden käytön.[20] s.13 Valtionhallinnon osalta tietoturvallisuudella suojataan organisaation omaa ja yhteiskunnan toimintaa, sekä tietosuojalla kansalaisten tietoja. Valtionhallinnon organisaatioiden toiminta ja päätöksenteko perustuu tiedon luotettavuuteen. Voidaan olettaa, että näin on myös muissa organisaatiossa. Tiedon suojaamisella teknisten ja käytännön tietoturvallisuuden toimintatavoilla mahdollistetaan kansalaisten tietosuojan toteutus ja yhteiskunnan tärkeiden toimintojen turvallisuus.[20] s.15



Kuva 2. Tietoturvallisuuden rakentuminen organisaatiossa

Tietoturvallisuuden toteutus organisaatiossa perustuu keskeisesti voimassa oleviin kansainvälisiin ja kansallisiin sopimuksiin, lakeihin ja normeihin. Tietoturvaratkaisuja toteuttaessa niiden noudattaminen on välttämätöntä. Lait velvoittavat organisaatioiden ja viranomaisten varmistumaan kaikessa toiminnassaan riittävästä tietoturvallisuuden tasosta sisäisessä ja ulkoisessa tiedonvaihdossa sekä valtiohallinnon ulkopuolisten organisaatioiden kanssa.[21]s.15-16 Organisaatioiden tietoturvan toteutukseen ja arkaluontoisten tietojen käsittelyyn vaikuttavat seuraavat lait:

- Laki kansainvälisistä tietoturvavelvoitteista (588/2004), joka velvoittaa kansainvälisessä yhteistyössä Suomea valtiona kunnioittamaan kansainvälisen yhteistyön turvallisuusvelvoitteiden noudattamista.
- Tietoturvallisuutta käsittelevät valtioiden väliset sopimukset sekä muut valtion hyväksymät kansainväliset turvallisuussäännöstöt.
- Perustuslaki, joka asettaa raamit tietoturva- ja tietosuojavaatimuksille (731/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (621/1999).
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, joka määrittelee salassa pidettävien tietojen käsittelyä (681/2010).
- Henkilötietolaki (523/1999), jolla suojataan perusoikeuksia henkilötietoja käsiteltäessä sekä edistetään hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.
- Laki sähköisen viestinnän palveluista eli niin sanottu tietoyhteiskuntakaari (917/2014)
- Laki sähköisestä asioinnista viranomaistyössä (13/2003) [21]s.15 [22]

Voimassa olevia sääntöjä, lakeja ja sopimuksia noudattaen organisaatio suorittaa riskienhallintaprosessin kaikkine toimenpiteineen saadakseen kattavan kuvan kaikista siihen ja sen toimintaan kohdistuvista riskeistä. Riskienhallinta tarkoittaa niitä organisaation suorittamia toimenpiteitä, joilla se johtaa, sekä ohjaa organisaation riskejä.[23]s.11-12 Riskienhallinnan tavoitteena on luoda menestyvä organisaatio, jonka toiminta on jatkuvaa ja asetetut tavoitteet saavutetaan. Oikein toteutettuna riskienhallinnalla on selkeät asetetut tavoitteet, joilla mahdollistetaan organisaation kehittyminen ja ennakoitu johtaminen.[23]s.12-13 [24]s.8-9

Tietoturvallisuus on yhteydessä riskienhallintaan tietoriskien arvioinnin kautta. Organisaatio arvioi tieto- ja tietoturvariskejä riskienarvioinnin ja toiminnansuunnittelun ohella. Tietoriskejä arvioidaan, organisaation perustehtävän ja sen saavuttamiseksi asetettujen strategioiden ja tavoitteiden kautta.[20] s.16 Riskienhallinta on osa johtamisen ja toiminnan prosesseja sekä suunnittelua ja seurantaa. Tavoitteena on, että organisaatiolla on johtamista ja päätöksentekoa varten ajantasainen, oikea ja riittävän kattava käsitys riskeistä sekä selkeästi määritellyt riskienhallinnan vastuut ja seurantajärjestelmä. Johtamisen ohella riskienhallinta koskettaa organisaation jokaista työntekijää; yksinkertaisimmillaan se tarkoittaa työntekijän omaan arvioon perustuen normaalista toiminnasta poikkeavien havaintojen ilmoittamista omalle esimiehelleen.[23] s.12

Riskienhallinnan tuotoksena on organisaation riskianalyysi, jolla se perustelee käytettävät tietoturvatoimenpiteensä ja – ratkaisunsa. Riskianalyysissä tietoturvariskit suhteutetaan lainsäädäntöön, toimintaympäristöön sekä kustannuksiin. Riskianalyysilla organisaatio selvittää sen tärkeimmät omaisuudet ja niihin kohdistuvat uhat. Riskianalyysin perusteella organisaatio arvioi vahingot, mikäli jokin tiedostetuista uhkista toteutuu ja budjetoi riittävät resurssit omaisuuden suojelemiseen. Resursseilla toteutetaan organisaatiolle turvallisuuspolitiikka, jolla annetaan suuntaviivat teknisen ja käytännön turvallisuuden toteutuksille. Turvallisuuden käytännöillä tunnistetaan, ylläpidetään ja kehitetään toimintoja, joilla tunnistetut riskit säilytetään hyväksyttävällä tasolla.[19] s.70–71 Tiedostaessaan omaan toimintaan kohdistuvat uhat ja riskit organisaatio kykenee reagoimaan niihin ennakoivasti käytännön toimenpiteillä. Riskiarvioinnin perusteella organisaatio määrittelee muun muassa päätelaitteille oikeat tietoturva-asetukset ja tarvittavat käyttöjärjestelmän kovennukset. Näiden toimenpiteiden jälkeen työntekijät ohjeistetaan, millä päätelaitteella sallitaan minkäkin suojaustason tietojen ja palveluiden käyttö.[21] s.57-59

Kattavan riskienkartoituksen jälkeen organisaatiolle luodaan tietoturvapolitiikka sekä tietoturvastrategia. Kokonaisuuksina ne kuuluvat osaksi organisaation muuta toiminta- ja tietohallintopolitiikkaa ja -strategiaa. Organisaation tietoturvapolitiikka on näkemys tietoturvallisuuden tavoitteista ja käytännön toteutuksesta, joka muodostuu voimassa olevista tietoturvanormeista ja normien käytäntöön panosta. Tietoturvapolitiikasta puhutaan myös joskus organisaation tietoturvaperiaatteena.[10] s.111 Organisaation johto määrittää tietoturvatoiminnan tavoitteet, toiminnan suuntaviivat ja vastuujaon tietoturvapolitiikassaan. Käytännön tietoturvaohjeistukset ja – suunnitelmat perustuvat johdon laatimaan tietoturvapolitiikkaan.[25] s.25–28 Organisaation tietoturvastrategia on tapa, jolla tietoturvapolitiikka jalkautetaan organisaation jokapäiväiseen toimintaan.[10] s.111 Tietoturvapolitiikkaa laatiessa huomioidaan organisaation toimiala, toiminnan tarkoitus, muu strategia sekä yleiset tavoitteet. Organisaation noudattaessa tai tavoitellessa tietoturvastandardin mukaista sertifiointia, on tietoturvapolitiikan oltava vaaditun standardin mukainen. Organisaation johto vastaa tietoturvapolitiikan ajantasaisuudesta päivittämällä sisällön säännöllisin väliajoin sekä tilanteissa, joissa organisaatiossa tapahtuu toiminnallisia tai rakenteellisia muutoksia.[25] s.25-28

Tietoturvallisuuden toteutuminen varmistetaan organisaatiossa selkeällä henkilökunnan rooleilla ja vastuuhenkilöiden nimeämisellä. Organisaation ohjeistuksen noudattamista on valvottava ja varmistettava henkilökunnan tietotaidon tasosta. Organisaation tietoturvallisuudesta ja sen organisoimisesta vastaa tietohallinto-osasto tietoturvapäällikön johdolla. Johdon tuella ja riittävillä resursseilla tietoturvatyö saavuttaa asetetut tavoitteet sekä organisaation tavoitellun hyödyn.[19] s.120-125

Henkilöstön onnistuneella turvallisuuskoulutuksella organisaatio luo edellytykset turvallisuustavoitteiden saavuttamiseksi. Organisaation henkilöstölle järjestetään tietoturvapolitiikkaan perustuva tietoturvakoulutus esimerkiksi organisaation tietoturvavastaavan tai ulkopuolisen koulutusorganisaation toimesta. Peruskoulutuksella perehdytetään koko henkilöstö organisaation tietoturvakäytäntöihin ja se on järjestettävä mahdollisimman nopeasti palvelussuhteen alkamisen jälkeen. Riippuen työntekijän kohderyhmästä, peruskoulutusta seuraava syvällisempi koulutus saattaa poiketa sisällöltään. On ymmärrettävää, ettei tietotekniikkahenkilöstölle ole järkevää järjestää saman sisältöistä koulutustapahtumaa kuin muulle henkilöstölle. Tietoturvakoulutuksen tukena oleva organisaation tietoturvaohjeistuksen on oltava ajantasainen, linjassa tietoturvapolitiikan kanssa ja sen mahdollisista muutoksista on ilmoitettava henkilöstölle. Tarvittaessa henkilöstölle järjestetään uusi koulutustilaisuus. Ohjeistuksen on oltava lyhyt, selkeä ja ennen kaikkea helposti noudatettavissa. On olemassa riski, että henkilöstö

jättää ohjeistusta noudattamatta, mikäli he kokevat sen haittavan tai hidastavan työntekoa.[26] s.21–25

Organisaation koko henkilöstölle järjestettävässä tietoturvaperuskoulutuksessa opetetaan esimerkiksi:

- Tietoturvatoiminnan tavoitteet, organisointi, vastuut ja tehtävänjako
- Noudatettava tietoturvaohjeistus
- Tietoturvan peruskäsitteet
- Viranomaisen toiminnan julkisuus ja salassapitovelvoitteet
- Asiakirjojen luokittelu ja käsittely
- Henkilötietojen käsittely
- Tietokoneen ja mobiililaitteiden käyttö
- Internetin ja sähköpostin käyttö
- Etätyö ja etäkäyttö
- Toiminta ongelmatilanteissa ja ilmoitusvelvollisuus [26] s.21-25

Organisaation suorittamien ennakoivien tietoturvatoimenpiteiden jälkeen tärkeässä roolissa on työntekijöiden oma arviointikyky.[19] s.125 Ciscon vuonna 2017 julkaisemassa Security Research-tutkimuksessa todetaan, että vastaamalla haavoittuvuuksiinsa vain teknisillä ratkaisuilla organisaatio kykenee estämään vain 26 prosenttia sitä vastaan kohdistuvista hyökkäyksistä. Loput 74 prosenttia voidaan estää vain organisaation politiikan ja henkilöstön avulla.[27] s.53 Näin ollen heidän on ymmärrettävä oma merkityksensä organisaation tietoturvan luomisessa. Esimerkiksi turvaluokitellun tiedon käsittelyyn liittyvät ohjeistukset ja käytännön toimenpiteet on tehty organisaation parhaaksi. Organisaation on tehtävä tiedon turvallisesta käsittelystä mahdollisimman sujuvaa, jotta työntekijät kokevat tietoturvallisen työnteon loogiseksi ja parhaimmassa tapauksessa helpoimmaksi tavaksi tehdä annettu työtehtävä.[15] s.69 [17]s.31-32

2.3. Käyttöoikeudet

Organisaation työntekijät muodostavat omalla toiminnallaan turvallisuusuhkia pyrkiessään käsiksi tietoon, johon heillä ei ole oikeutta.[28] s.230 Oikeanlaiset käyttöoikeudet lisäävät tietoturvallisuutta. Päätelaitteiden puutteita suojauksessa voidaan vahvistaa tietojärjestelmän teknisillä ratkaisuilla tai tietojen käsittelyn rajoituksilla, eli toisin sanoen käyttöoikeuksien avulla.[21] s.33 Käyttöoikeuksien kontrollointi on mahdollista henkilökohtaisten kirjautumistunnusten avulla. Kirjautumisen valvonnalla hallinnoidaan pääsyä organisaation palveluihin. Tietojärjestelmään kirjautuminen voidaan yksinkertaisimmillaan toteuttaa työntekijän yksilöl-

lisen käyttäjätunnuksen ja salasanan yhdistelmällä. Tunnistuksen tehostamiseksi ja mahdollisten väärinkäytösten minimoimiseksi edellä mainittujen asioiden ohella voidaan käyttää sirullisista toimikorttia tai biometristä-tunnistusta. Kirjautumishetkellä valvontaa toteuttava tietojärjestelmä tarkistaa käyttäjän käyttäjätiedot sekä käyttöoikeudet, päästäen henkilön käyttöoikeuksien mahdollistamaan tietoon käsiksi.[18] s.124

Käyttöoikeuksien antamisen lähtökohtana on työnteon mutkaton toteuttaminen. Organisaatioissa on yleensä perustoimenpiteenä antaa user-tason eli peruskäyttäjän oikeudet sen työntekijöille. Tarvittaessa oikeuksia laajennetaan yksilökohtaisesti, jotta sujuva työnteko onnistuu. User-tasosta korotetuilla oikeuksilla käyttäjä lisää tietoturvauhkia omalla toiminnallaan, oli se sitten tahallista tai tahatonta. Korotetut oikeudet käyttäjällä mahdollistavat esimerkiksi sovellusten asennuksen muualta, kuin virallisista lähteistä, sekä antavat mahdollisuuden palveluille kuunnella verkkoa ja lähettää tietoja päätelaitteesta muualle.[21] s.23 Järvisen ja Rouskun mielestä suurimmalle osalle työntekijöistä riittää käytettävään työasemaan pelkät perusoikeudet. Rajoittamalla työntekijöiden käyttöoikeuksia, organisaatio pystyy tehokkaasti estämään tahalliset ja tahattomat vahingot. Tämä on toimiva ratkaisu myös työntekijän käyttäessä itsekustantamaansa päätelaitetta työntekoon.[17] s.104–105 Perusoikeuksilla jokapäiväisten työtehtävien suorittaminen on mahdollista. Niillä kyetään päivittämään käyttöjärjestelmä sekä muokkaamaan tarpeelliset työpöydän asetukset. Antamalla työntekijöille peruskäyttöoikeudet päätelaitteelle ja järjestelmiin estetään verkko-asetusten muokkaaminen, omien oikeuksien laajentaminen, toisten käyttäjätunnusten muokkaaminen, käyttöjärjestelmän toiminnan muokkaaminen sekä ennen kaikkea estetään pääsy käsiksi tietoihin, joihin työntekijän ei tarvitse päästä. Näin organisaatio pienentää omaa hyökkäyspinta-alaansa.[21] s.40 Hyökkäyspinta-ala tarkoittaa järjestelmän tai esimerkiksi sovelluksen osaa, jota vastaan hyökkääjä voi kohdistaa toimenpiteensä. Mitä vähemmän heikosti suojattuja osia on, sitä parempi tilanne on organisaatiolle. Sen ei ole järkevää laajentaa hyökkäyspinta-alaansa muulloin kuin hyvin perusteltuna.[19]s.1099 Mikäli työntekijän käyttäjätunnus ja salasana päätyvät ulkopuoliselle, on tilanne helpoin hallita työntekijän käyttöoikeuksien rajoittuessa user-tasolle. Tällöin vahingon laajuudet saadaan minimoitua, koska käyttöoikeudet eivät salli juurikaan minkään tason muutoksia järjestelmässä.[29]s.602 Haittaohjelman päästessä peruskäyttäjän päätelaitteelle, ei se pysty tehokkaasti vaikuttamaan näihin estettyihin asetuksiin ja sisältöihin. Toisin sanoen rajoitetut käyttöoikeudet suojaavat itse käyttäjää sekä organisaatiota haittaohjelmien vahingoilta.**Virhe. Viitteen lähdettä ei löytynyt.** Valtiovarainministeriön julkaisemassa VAHTI-ohjeessa esitellyssä kyselytutkimuksessa esimerkki organisaation työntekijöiltä kysyttiin, mitä sovelluksia he haluavat käyttää omilla laitteillaan. Työntekijät halusivat pääasiassa käyttää sähköpostia, kalenteria sekä organisaation dokumenttien hallintajärjestelmää. Tutkimuksen

yhteydessä tehtiin havainto, etteivät työntekijöiden toiveet ole toteutettavissa ilman omien laitteiden valvontaa.[21]s.65

2.4. Organisaatioon kohdistuvat tietoturvauhat

Organisaatioihin kohdistuu tietoturvauhkia eri syistä, sekä eri tahojen toimesta. Organisaation omistamalla, ei yleisessä jaossa olevalla tiedolla, voi olla useita käyttötarkoituksia. Viestintäviraston kyberturvakeskuksen ja sen yhteistyöverkostojen yhteisarvion perusteella Tietoturvan vuosi 2017-julkaisussa organisaatioiden viideksi suurimmaksi uhiksi tietoturvan osalta ovat päätelaitteiden päivitysten laiminlyönti, kiristyshaittaohjelmat, tietoja kalastelevat huijausviestit, ulkoistusten ja laitehankintojen hallinta sekä hyökkäysuhkaukset.[30]s.5 Julkaisun mukaan suurimmat uhat ovat olleet samansuuntaisia jo muutaman vuoden ajan.

Päätelaitteiden päivitysten laiminlyönti luo vihamieliselle taholle hyvät mahdollisuudet hyökkäyksen onnistumiselle. Laite, joka ei ole ajantasaisesti päivitetty sisältää vakavia haavoittuvuuksia ja on hyvä alusta haittaohjelmien, hyökkäysten ja tietomurtojen nopealle leviämiselle.[30]s.5 Oppliger määrittelee haavoittuvuuden tietoteknisen järjestelmän viaksi tai heikkoudeksi sen suunnittelussa, toteutuksessa, toiminnossa tai hallinnassa, jota hyväksikäyttämällä rikotaan järjestelmän turvallisuuskäytäntöjä.[31]s.8

Päivitysten asentamisen merkitys korostuu toukokuussa 2017 organisaation sisäverkossa nopeasti levinneestä WannaCry-kiristyshaittaohjelmasta. Perjantaina 12. toukokuuta alkaneessa hyökkäyksessä noin 200 000 tietokonetta 150 maassa altistui kyseiselle haittaohjelmalle. Tietokoneen tiedostot salattiin ja käyttäjältä vaadittiin 300 dollarin lunnaiden maksamista purkuavainta vastaan. Maksetut lunnaat ovat rikollisille merkittävä tulonlähde, jonka vuoksi kiristyshaittaohjelmia esiintyy. WannaCry hyödynsi Windowsin SMB-verkkoprotokollan haavoittuvuuksia, johon Microsoft oli julkaissut päivityksen kaksi kuukautta ennen kiristyshaittaohjelman leviämistä. WannaCrylle altistuneissa organisaatioissa oli käytössä Windows XP:n käyttöjärjestelmän versioita, jotka eivät olleet enää päivitysten piirissä ja tästä syystä organisaatiot altistuivat haittaohjelmalle. Kiristyshaittaohjelman leviäminen saatiin pysäytettyä 18. toukokuuta rekisteröimällä WannaCryin hyödyntämä verkko-osoite. Maailmalla kiristyshaittaohjelma sai vaurioita aikaan vaikuttaen muun muassa sairaaloiden toimintaan Englannissa. Kyberturvallisuuskeskuksen mukaan vain kymmenisen organisaation verkossa havaittiin WannaCry-tartunta. Tästä syystä vauriot jäivät Suomessa pieniksi.[30]s.8

Yksittäisiin henkilöihin tai ryhmiin kohdistettavilla tietojen kalasteluviesteillä pyritään saamaan haluttua tietoa organisaatiosta. Tietojen kalasteluun hyödynnetään muun muassa sähköpostipalvelua.[19] s.271 Työntekijöitä lähestytään sähköpostitse esittäytyen esimerkiksi tietohallinnon edustajana ja vaaditaan vaihtamaan salasanansa avaamalla sähköpostiviestissä oleva linkki, joka avautuu oikean näköiseksi verkkosivustoksi. Vaihtaessaan salasanansa työntekijä luovuttaa sekä nykyisen salasanansa että käyttäjätunnuksensa ulkopuoliselle, joka voi hyödyntää sitä haluamallaan tavalla.

Organisaatiot ovat ulkoistaneet IT-ylläpitopalveluitaan ja laitehankintojaan saavuttaakseen tehokkuutta sekä taloudellisia säästöjä. Ulkoinen IT-palvelutarjoaja on kiinnostava hyökkäyskohde rikollisten näkökulmasta, koska se on yhteistyössä useiden organisaation kanssa ja sillä on pääsy näiden tietoverkkoihin. Ulkoistus säästää resursseja, mutta uhka myös sen kautta on mahdollinen. Lähivuosina on yleistynyt tapa, jolla organisaatiota kiristetään uhkaamalla tietomurrolla tai muilla hyökkäyksillä. Uhkaus harvemmin toteutuu, koska sen on tarkoitus aiheuttaa pelkoa organisaation johdossa ja saada heidät maksamaan tietty summa uhkauksen tekijälle.[30]s.5

Voidaan olettaa, että organisaatio on rakentanut tietoverkkonsa mahdollisimman tietoturvallisiksi tarvittavien teknisten kokonaisuuksien ja tietoturvastandardien mukaisesti. Yksittäinen henkilö eli organisaation työntekijä omilla toimillaan ja ratkaisuillaan on keskiössä organisaation tietoturvan luomisessa ja valitettavan usein työntekijä on tietoturvakokonaisuuden heikoin lenkki. Tästä syystä vihamieliset tahot kohdistavat usein hyökkäyksensä organisaatiossa yksittäisiin henkilöihin tai ryhmiin, kuten edellä mainittiin. Hyökkäyksillä voidaan pyrkiä saamaan haltuun kirjautumistunnuksia ja organisaatiolle kriittisiä, salassa pidettäviä tietoja. Hyökkäys voidaan toteuttaa esimerkiksi seuraavilla tavoilla:

- Käyttäjän ennestään saastutettu ulkoinen laite liitetään verkkoon ja liittämishetkellä haittaohjelma siirtyy organisaation järjestelmiin. Ulkoinen laite voi olla esimerkiksi USB-tikku tai älypuhelin
- Käyttäjää lähestytään sähköpostilla tai sosiaalisen median kautta ja pyydetään avaamaan liitetiedosto tai linkki, jonka avaamalla haittaohjelma asentuu
- Sähköpostitse voidaan lähestyä esimerkiksi ylläpidon elementissä ja pyydetään vaihtamaan salasana aidon näköisessä sivustossa. Todellisuudessa käyttäjä luovuttaa tunnuksensa ja salasanansa ulkopuoliselle
- Päätelaitteessa olevaa haavoittuvuutta hyödynnetään ja laitteelle luodaan etäyhteys
- Perinteisesti haitallisella verkkosivulla vierailleminen

MITM-hyökkäyksellä eli hyökkääjä esiintyy esimerkiksi organisaation langattomana verkkona, jolloin työntekijän liittyessä verkkoon hän on yhteydessä organisaation WLAN-verkkoon samalla kun hyökkääjä on käyttäjän ja verkon välissä saaden kaiken työntekijän käyttämän tiedon[21] s.21–22

2.5. Hyökkääjät

Järvinen ja Rousku jakavat organisaatioiden tietoverkkoihin iskevät tahot viiteen kategoriaan: harrastelijoihin, niin sanottuihin haktivisteihin, tietoverkkorikollisiin, kyberterroristeihin sekä valtiolliseen tiedusteluun. [17] s.33 Harrastelijoiden toiminta perustuu omien kykyjen kokeiluun sekä alan piireissä maineen hankintaan. Tekijät eivät välttämättä tiedosta tekojensa olevan rikosoikeudellisesti tuomittavia.[17] s.33–34 Haktivistit hyödyntävät viimeisintä teknologiaa omien tarkoitusperiensä edistämiseen. Organisaatioihin kohdistetaan laittomia sekä niin sanottuja harmaan alueen toimia. Haktivistit kohdistavat toimensa viranomaistahoihin tai organisaatioihin harjoittaen esimerkiksi sähköpostipommituksia tai palvelunestohyökkäyksiä.[17] s.34–35 Tietoverkkorikollisten toiminnan tarkoituksena on oman taloudellisen hyödyn saaminen. Yksi tapa on saada organisaatiolta tietoja, jotka ovat itsessään taloudellisesti arvokkaita. Tietoa voidaan esimerkiksi myydä eteenpäin siitä kiinnostuneelle taholle.[17] s.35–36 Tietoverkkorikollisina kyberterroristit kohdistavat iskunsa organisaation tietoliikenneverkkoihin tai ICT-palveluihin, tarkoituksena niiden lamauttaminen tai mahdollisimman suuren vahingon tuottaminen. Yksittäisen organisaation ohella iskut voidaan kohdistaa yhteiskunnan kriittisiin palveluihin, kuten sähkönjakeluun tai terveydenhuoltopalveluihin. Valtiollisella tiedustelulla tavoitellaan oman kansallisen edun saavuttamista sotilaallisessa, taloudellisessa, poliittisessa tai muussa mielessä.[17] s.37 Tietoverkkorikolliset ja kyberterroristit hyökkäävät organisaatioihin tavoitteenaan käyttäjätunnusten, salasanojen, henkilö- tai luottokorttitietojen varastaminen sekä kiristäminen tai palvelun estäminen. Hyökkäykset voidaan toteuttaa huijaussähköposteilla, palveluihin murtautumalla tai tietoja varastamalla.[17]s.37

3. BRING YOUR OWN DEVICE

3.1. BYOD käsitteenä

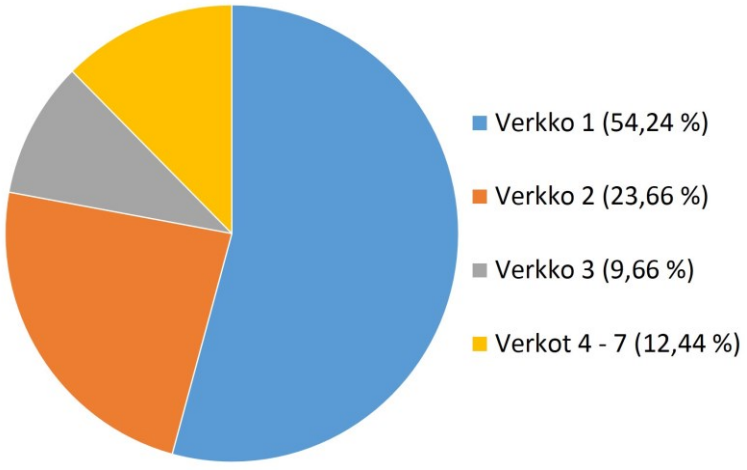
Bring Your Own Device käsitteenä on osa laajempaa yritysmaailmassa tapahtuvaa ilmiötä, IT-kuluttajistumista (consumerization of IT) Ilmiöllä tarkoitetaan organisaation jäsenen, esimerkiksi työntekijän halua tuoda omat, itsekustantamansa päätelaitteet työpaikalle ja valjastaa käytössä olevat erikois- sekä sosiaalisen median-sovellukset osaksi jokapäiväistä työntekoa.[32]s.99 Trendin alkuaikoina työntekijät alkoivat käyttää vapaa-ajalle suunniteltuja sovelluksia ja chat-ohjelmia työnteon yhteydessä. Bring Your Own Device-toimintatapa eroaa IT-kuluttajistumisilmiöstä siten, että työntekijän tahtotila muuttuu teoksi. Bring Your Own Device-ilmiön osana on työnantajan suostumus, jolla oman päätelaitteen käyttö sallitaan organisaation tietoverkossa.[33] s.21–23 Työntekijä omistaa viihde ja kommunikointikäyttöön hankitun päätelaitteen, jonka käyttö ja toiminnallisuudet ovat hänellä hyvin hallussa. Käyttäessään omistamaansa päätelaitetta työntekoon, puhutaan BYODista. Tuttu käyttöympäristö sovelluksineen ja työkaluineen mahdollistaa tehokkaan työnteon. Voidaan olettaa, että vapaa-ajan laitetta hyödynnetään jo työntekoon jollakin tasolla, kuten sähköposti- tai kalenteritoimintojen osalta. BYOD poistaa työntekijöiltä kahdella laitteella työskentelemisen.[34] On ymmärrettävää, ettei työntekijä halua kantaa useampaa älypuhelinta mukanaan töitä tehdessään.

BYOD käsitettä ja siihen liittyvää vastuuta ei välttämättä ymmärretä täysin oikein, syynä voidaan pitää sen aihepiirin teknisyyttä. Puhuttaessa tietotekniikasta ja teknisistä laitteista, ne mielletään usein koskevan vain IT-alaa, ei omaa jokapäiväistä toimintaa. Organisaation on koko laajuudessaan asennoiduttava BYOD-käytäntöön eikä se saa jäädä IT-sektorin työtaakaksi. Kyse on kuitenkin tavasta tehdä työtä, eikä pelkästä tekniikasta.[35] BYOD-laitteella käsitellään työnteossa tarvittavia organisaation tietoja. Tieto itsessään voi sijaita kyseisellä päätelaitteella, organisaation sähköisissä tietojärjestelmissä tai muissa palveluissa, kuten pilvipalveluissa.[16] s.194–195 Bring Your Own Device-toimintatapa käsitteenä kattaa alleen työntekijän henkilökohtaisesti kustantamat laitteet, joilla on pääsy organisaation tietoverkkoon ja on teoreettisesti mahdollista tehdä töitä. Laitteen on kyettävä muodostamaan verkkoyhteys ja siinä on oltava näyttöpääte, jonka kautta työntekijä hallitsee tiedostojen lukemista sekä muokkaamista esimerkiksi kirjoittamalla.

3.2. BYOD organisaatiossa

Työntekijöiden henkilökohtaisen päätelaitteen tuominen töihin ja laitteella liittyminen organisaation tietoverkkoihin tuo ilmiö mukanaan organisaation kannalta niin hyötyjä kuin haasteita. BYOD-toimintatavan myötä organisaatioiden tulee hyväksyä tosiasia, että työntekijöiden erilaiset ja jatkuvasti kehittyvät laitteet pyrkivät yhdistymään sen tietoverkkoihin, tietoon ja sovelluksiin. Haaste ei näy poistuvan, vaan siitä muodostuu osa organisaatioiden päivittäistä toimintaa, halusivat organisaatiot sitä tai ei. Omien laitteiden käyttö pitää sovittaa osaksi organisaation toimintaa, jotta siitä saataisiin paras mahdollinen hyöty. [3] BYOD-toimintatavan myötä organisaatioiden IT-infrastruktuuri on muuttunut suljetusta avoimeen. Työntekoon tarvittavaan tietoon ja palveluihin on nykyään mahdollista päästä käsiksi mistä tahansa, toimivan internet-yhteyden välityksellä. Suljetussa ympäristössä tieto oli käytössä vain organisaation hallinnoimilla päätelaitteilla, kun BYOD-laitteiden myötä tieto voi sijaita myös organisaation ulkopuolella.[36]s.1

Tarkastellaan organisaatiota, jossa on käytössä seitsemän langatonta verkkoa. Osa verkoista on luotu jokapäiväiseen työskentelyyn, osa organisaatiossa vierailevien ulkopuolisten henkilöiden tarpeisiin. Kyseisessä esimerkki-organisaatiossa verkkojen käyttäjille jaetaan päivittäiseen työskentelyyn päätelaitteet talon puolesta. Alla olevassa kaaviossa näkyy langattomien verkkojen käyttöaste tavallisena arkipäivänä, jolloin verkkojen käyttö on normaalilla tasolla. Alkuperäinen organisaation tietohallintoalalta saatu näkymä langattomien verkkojen käytöstä on tutkijan hallussa. Tässä yhteydessä organisaation mainitsemista ei koeta tärkeäksi.



Kuva 3. WLAN-verkkojen käyttöasteet esimerkkiorganisaatiossa.[37]

Esimerkki-organisaatiossa kolme käytetyintä WLAN-verkkoa ovat:

- Verkko 1 (54,24 %), joka on BYOD-käyttöön suunniteltu WLAN-verkko.
- Verkko 2 (23,66 %), joka on organisaation suurimmalle henkilöstöryhmälle suunniteltu WLAN-verkko.
- Verkko 3 (9,66 %), joka on organisaation vieraille suunniteltu WLAN-verkko.

Verkko 1:ssä on eniten liikennettä ja käyttäjiä tavallisena arkipäivänä. Prosenttiosuutta nostaa työntekijöille jaetut työasemat, joita verkkoon on myös liittyneenä, mutta lähtökohtaisesti liikenne koostuu verkon käyttäjien henkilökohtaisista päätelaitteista. Organisaation tarjoama BYOD-WLAN on suuresta käyttöasteesta huolimatta mobiililaitteiden käyttämiä 4G-yhteyksiä nopeampi, joka selittää myös verkon suosiota.

Seuraavaksi tarkastellaan Bring Your Own Device-toimintatavan hyötyjä ja haasteita. Vaikutuksia käsitellään organisaation ja yksittäisten työntekijän näkökulmista. Hyötyjen ja haasteiden esilletuomisen avulla tutkielmassa tuodaan esille BYOD-käsitteen laajuus ja siihen liittyviä asiakokonaisuuksia. Tutkimuksessaan Voltti nostaa esille IT-kustannusten muutoksen, jonka positiivisista vaikutuksista organisaation sisällä löytyy mielipiteitä puolesta ja vastaan.[12]s.22 Näkökulmasta riippuen organisaatio voi kokea eri tavalla, onko tapahtunut muutos hyöty vai haitta. Organisaatiolle BYOD tuo uutena toimintatapana suuren määrän haasteita, jotka eivät ole ylitsepääsemättömiä, mikäli riskit tunnistetaan ja niiden varalta on laadittu organisaatiolle ajantasainen ohjeistus.

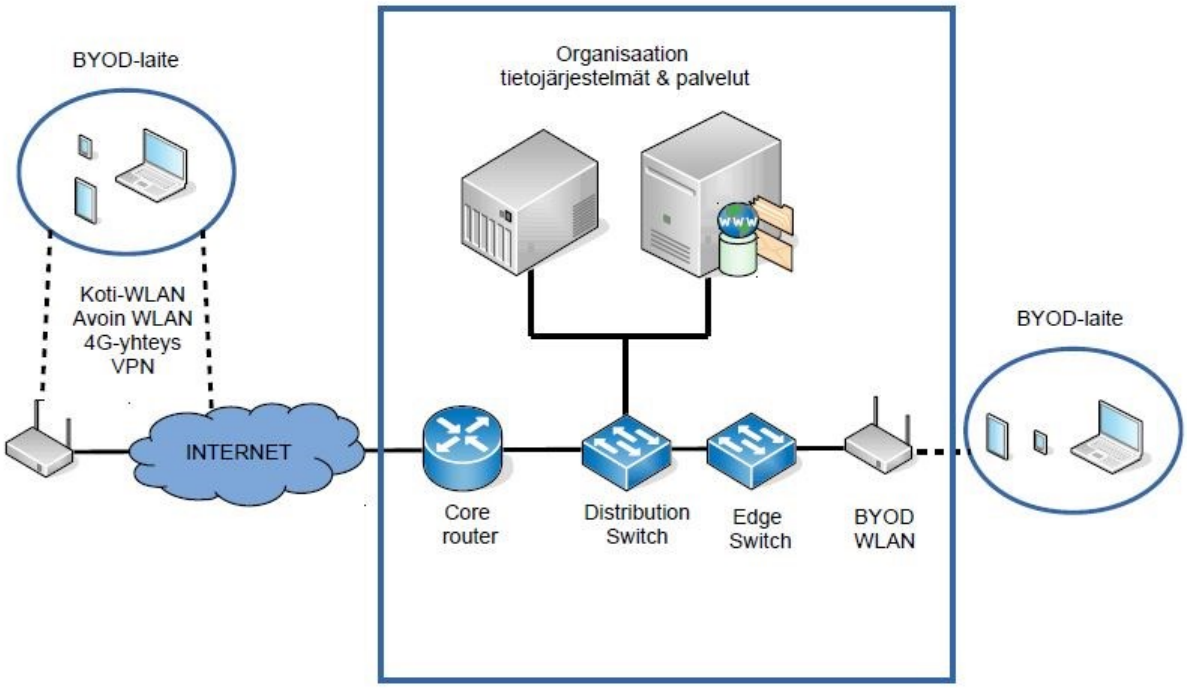
3.3. BYOD-laite

Tutkimuksessa BYOD-laitteella tarkoitetaan verkkoyhteydessä olevaa päätelaitetta, jolla käsitellään organisaation tietoa. Tarkasteltavina laitteina ovat älypuhelin, tabletti sekä kannettava tietokone niiden ollessa mobiileja laitteita, joiden käyttäminen BYOD-tarkoitukseen on järkevintä. Yhteyden organisaation verkkoon BYOD-laite saa muodostamalla yhteyden internetiin verkkokaapelin kautta tai langattomasti liittymällä organisaation toimitiloissa olevaan BYOD WLAN-verkkoon. Liittyminen organisaation verkkoon ohjeistetaan työntekijöille BYOD-ohjeistuksessa. BYOD-laitteen ollessa fyysisesti organisaation WLAN-verkon kantaman ulkopuolella, voidaan yhteys muodostaa vaihtoehtoisesti 4G-verkon tai toisen WLAN-verkon kautta.

Tietoliikenneverkkoja on kolmen tyyppisiä:

- avoimia, kuten internet
- puoliavoimia, kuten organisaatioiden sisäverkot sekä
- kokonaan suljettuja, jotka ovat yleisesti sotilaskäyttöön suunniteltuja.[38]s.129

BYOD-laitteella liityttäessä osaksi organisaation verkkoa yhteyden sekä päätelaitteen ja organisaation pään suojausmekanismit on oltava kunnossa riskien minimoimiseksi. Päätelaitteelta tapahtuvaa tietoliikenteen suojausmekanismeja ovat muun muassa VPN eli Virtual Private Network. Teknisenä ratkaisuna organisaatio voi vaatia VPN-yhteyden käyttöä liityttäessä sen tietojärjestelmiin ulkopuolisella internet-yhteydellä.[36]s.2 VPN-yhteys tarkoittaa niin sanotun turvallisen liikennöimistunnelin muodostamista päätelaitteen ja organisaation palomuurien välille tuntemattomien verkkojen, kuten internetin yli. VPN-yhteyden käyttämät salaus- ja tunnelointiprotokollat turvaavat tiedon luottamuksellisuuden ja eheyden eristämällä päätelaitteen liikennöinnin muusta internetin liikenteestä, tehden yhteydestä turvallisemman, niin työntekijän kuin organisaation kannalta. [31]s.139 [19]s.702 VPN-yhteys turvaa arkaluontoisten tietojen liikennöinnin päätelaitteiden ja verkkojen välillä. Useat tietoturvayhtiöt tarjoavat kohtuulliseen hintaan VPN-ohjelmia niin mobiililaitteille kuin perinteisille tietokoneille.



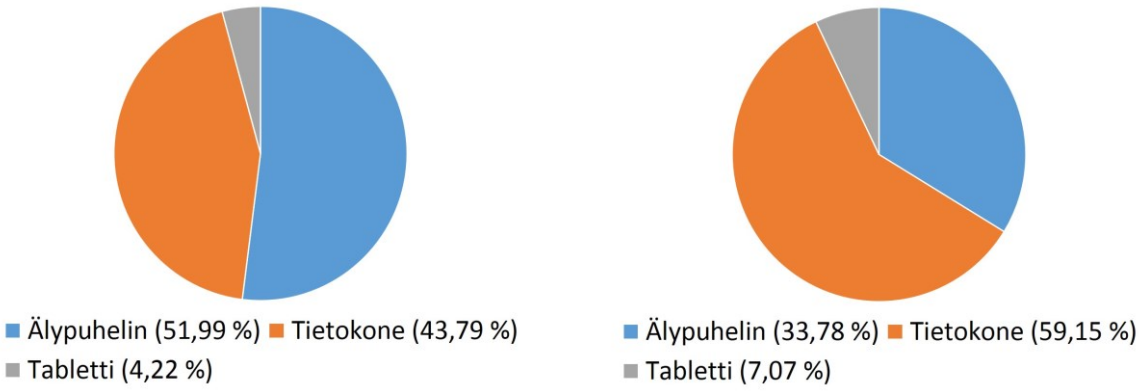
Kuva 4. BYOD-laitteen tietoliikenneyhteyden toteutus. Mukaillen[36]s.2

BYOD-laitteet käyttävät tietoliikenneyhteyksien muodostamiseen edellä mainittujen WLAN- ja 4G eli LTE-tekniikan lisäksi myös seuraavia tekniikoita:

- 2G eli GSM
- 3G eli WCDMA
- Ethernet
- Bluetooth
- NFC
- RFID [21]s.24-25

Tietoliikennetapojen turvallisuuksissa on eroja, mutta oikein tehtynä ne mahdollistavat suojatun ja turvallisen liikennöinnin jopa suojaustason IV tietoja käsitellessä, esimerkiksi WLAN-yhteys mahdollistaa tämän. Riskiarvioinnissa organisaation on hyvä selvittää yhteystapojen heikkoudet muun muassa salauksen osalta ja selvitetään millaisilla toimenpiteillä ne voidaan toteuttaa turvallisesti. Riskiarvioinnin perusteella organisaatiossa tehdään päätös, mitkä yhteystavat sallitaan työntekoon.[21]s.24

Edellä mainitut BYOD-laitteen ominaisuudet täyttävistä päätelaitteista, yleisimmät ovat älypuhelin, tabletti sekä kannettava tietokone. Tarkasteltaessa näiden kolmen päätelaitetyypin markkinaosuuksia kuvassa 5, koko maailmassa ja Suomessa, on havaittavissa muutama asia. Älypuhelinten määrä maailmassa on ohittanut tietokoneet, niin pöytä- kuin kannettavatkin mallit. Älypuhelinten yleistymisen trendi on havaittavissa myös Suomessa, missä tietokoneet ovat yleisimpiä. Vuoden 2017 aikana älypuhelinten markkinaosuus kasvoi 9,09 prosenttia. Markkinaosuutta älypuhelimet ovat vieneet tietokoneilta.[39] Voidaan karkeasti yleistää, että älypuhelinten yleistyminen näkyy myös BYOD-laitteiden määrissä.



Kuva 5: Päätelaitteiden markkinaosuudet tammikuussa 2018. Vasemmalla maailma [40] , oikealla Suomi[39]

BYOD-laitteina älypuhelin ja tabletti eroavat kannettavista tietokoneista käsittelyominaisuuksiltaan. Älypuhelimen ja tabletin käyttöprofiili perustuu kosketusnäyttöön, jolla on helppo selata internetiä, lähettää lyhyitä pikaviestejä ja ottaa esimerkiksi valokuvia. Tämän kaltaisissa suoritteissa kosketusnäytölliset päätelaitteet ovat vahvimmillaan. Kannettava tietokone on näppäimistönsä takia selkeästi parempi tiedon tuottamiseen kuin mobiililaite. Kaikenlaisen median selaamiseen kannettava sopii myös erinomaisesti. BYOD-laitteiden käyttöjärjestelmistä ja niiden tietoturvaeroista kerrotaan neljännessä pääluvussa.

Älypuhelimille, tableteille sekä kannettaville tietokoneille tallentuu tietoja automaattisesti käyttäjän itsensä tallentamien tiedostojen lisäksi. Automaattisesti tallentuvien paikallisten tietojen tarkoituksena on nopeuttaa käytettävän palvelun toimintaa. Näitä ovat muun muassa varmuuskopiot, väliaikaistiedostot, järjestelmän ja selaimen tunniste- sekä sijaintitiedot, sovelluksiin sekä sovelluksista päätelaitteelle tallentuvat tiedot, sekä kirjautumistiedot, kuten käyttäjätunnukset ja salasanat, mikäli käyttäjä sen sallii. Loppukäyttäjä ei varsinaisesti näe näiden tietojen olemassaoloa kuin päätelaitteen käyttömukavuuden lisääntymisellä. Päätelaitteen ei tarvitse suorittaa kaikkia prosesseja alusta, vaan tarvittavat tiedot ovat jo olemassa, jolloin palvelu on nopeakäyttöisempi. Automaattisesti tallentuvat tiedot lisäävät tietoturvariskejä, joiden kohteena on erityisesti tiedon eheys.[21]s.23-24

Päätelaitteiden, käyttöjärjestelmien sekä sovellusten tietoliikennetoteutuksista löytyviä haavoittuvuuksia voidaan käyttää reittinä päätelaitteelle murtautumiseen. Zaidi et al. mukaan suurin osa älypuhelimiin kohdistuvien hyökkäysten taustalla ovat niiden haavoittuvuudet. Mikäli haavoittuvuudet saadaan minimoitua, niin käy myös hyökkäyksille. Älypuhelimien ajantasaisilla päivityksillä tämä on mahdollista.[41]s.216 Saatuaan päätelaitteen kokonaan tai osittain haltuunsa voi niin sanottu hyökkääjä esimerkiksi kuunnella laitteen mikrofonia tai muokata organisaation osalta salaisia tai muulla tavalla tärkeitä tietoja ja tiedostoja.[21]s.39

Zaidi et al. jakavat mobiililaitteisiin kohdistuvien hyökkäysten syyt kolmeen ryhmään:

- Arkaluontoisen tiedon saaminen. Mobiililaitteista on tullut henkilökohtaisten tietojen tallennuspaikkoja. Siksi niistä on tullut kiinnostavia hyökkäyskohteita vihamielisille tahoille. Hyökkäyksellä pyritään vahingoittamaan tiedon luottamuksellisuutta ja eheyttä. Onnistunut mobiililaitteeseen kohdistettu hyökkäys antaa hyökkääjälle pääsyn laitteen viesteihin, sähköposteihin, puhelu- ja yhteystietoihin.

- Laskentakyvyn hyväksikäyttö. Nykyaikaisten älypuhelimien laskentakyky ja –kapasiteetti kasvavat jatkuvasti, joka luo enemmän mahdollisuuksia laajemmille hyökkäyksille.
- Haitallinen ja vahingollinen toiminta. Joidenkin haittaohjelmien tarkoitus on tuottaa käyttäjälle epämukavuutta hyödyntäen hyökkääjän hyötymisen sijaan.[41]

3.4. Hyödyt

Voltin mukaan yritysten ja organisaatioiden merkittävimmät hyödyt BYOD-trendin myötä liittyvät henkilökunnan työtyytyväisyyden sekä työn joustavuuden, tehokkuuden ja liikkuvuuden paranemiseen.[12] s.48 Voltin tutkimuksen perusteella yritykset saavuttaisivat edellä mainitut hyödyt, mikäli toteutus on oikeanlainen ja se on yhteen sovitettu yrityksen strategian sekä liiketoiminnan kanssa.[12] s.63 Oman laitteen käyttö mahdollistaa etätöiden teon kotoa tai kaupungilta käsin huomattavasti paremmin tai vaihtoehtoisesti laitteen avulla yhteys perheenjäseniin ja ystäviin onnistuu helpommin.[7] Ympäröivän maailman tulo osaksi työn tekoa keventää työnteon ilmapiiriä ja vaikuttaa näin työntekijöiden tehokkuuteen. Motivaatio pysyy hyvällä tasolla, eikä töitä koeta raskaiksi. Lundenin ja Mattssonin tutkimuksessa hyödyiksi todettiin myös, että BYOD lisää työntekijöiden viihtyvyyttä sekä työmoraalia ja näiden kautta työn tehokkuutta. Tutkielmassa kuitenkin todettiin, että organisaation on ohjeistettava henkilökohtaisten laitteiden käyttö tarkasti riskien minimoimiseksi.[13]s.46-47

Organisaatiolle BYOD on taloudellisesti kannattava toimintatapa. Laitehankintojen siirtyessä työntekijöille organisaatio säästää taloudellisesti suuriakin summia, erityisesti lisenssikustannuksissa. Päätelaitteet uusiutuvat kuitenkin jatkuvasti ja suuremmalle organisaatiolle isojen laitemäärien hankinta tai liisaaminen käy kalliiksi. Säästösyistä laitehankinnoissa tyydytään kompromisseihin eikä välttämättä hankita parasta markkinoilla olevaa laitetta. Työntekijät haluavat mahdollisimman tehokkaan laitteen ja panostavat mielellään kalliimpaan laitteeseen kuin työnantajaorganisaatio.[34] Hankintapuolella syntyy säästöjä samalla kun työntekijällä on mahdollisesti parhain markkinoilta saatava laite.[3]

Hyödyt painottuvat taloudellisten säästöjen lisäksi erityisesti työntekijöiden viihtyvyyteen ja työnteon vapauteen sekä edellä mainittujen kautta yksittäisten henkilöiden motivaatioon, jonka seurauksena organisaation tehokkuus kasvaa. Lähtökohtaisesti parhaan mahdollisen tuloksen tekeminen on organisaatioiden tavoitteena, jota BYOD auttaa saavuttamaan motivoimalla työntekijät parempiin suorituksiin. Potentiaalia Bring Your Own Device-ilmiössä on, jonka luulisi kiinnostavan organisaatioita tuloksen saavuttamisessa.

3.5. Haasteet

Henkilökohtaisten laitteiden käyttäminen työntekoon muodostaa useita haasteita organisaatioille. Haasteiksi koetaan tietoturva, BYOD-laitteiden hallinta, palveluiden laadun säilyminen sekä laitteiden käyttöoikeuksien määrittely, eli mitä oikeuksia kullakin työntekijällä laitteellaan on. Palveluiden toimittajat, kuten ohjelmisto- ja sovellusvalmistajat tarjoavat mahdollisuuksia henkilökohtaisten laitteiden parempaan identifiointiin ja samalla käyttöoikeuksien määrittelyyn verkkoon liittymisen yhteydessä.[3] Haasteeksi muodostuu tiedon omistajuus, eli kuinka henkilökohtaiset ja organisaation tiedot kyetään pitämään erillään.

Organisaation tietoturvallisuudelle BYOD-laitteiden käyttöjärjestelmä ja yritystoimintaan räätälöityjen mobiilisovellusten kehittäminen ovat vakavimmat haasteet.[35] Organisaation salliessa henkilökohtaisten laitteiden käytön yrityksen toiminnassa, tulee sen toteuttaa automatisoituja toiminta- ja menettelytapoja. Edellä mainituilla toimilla organisaatio varmistaa, että työntekijällä on oikeat käyttöoikeudet ja hän noudattaa johdon vaatimia tietoturvaohjeistuksia laitteen käytön osalta.[35] Mikäli päätelaite on täysin työntekijän hallinnassa, ei työnantajalla ole oikeutta asentaa käyttäjän laitteeseen tietoturvallisuutta parantavia asetuksia ja ohjelmia keskitetysti, vaan käyttäjän on itse suoritettava tarvittavat päivitykset. Näitä ovat muun muassa palomuurit, haittaohjelmien torjunta, salaus sekä etähallinta. Laitteen hallinnan puuttuessa organisaatio ei voi varmistua päätelaitteen turvallisuudesta. Kun turvallisuudesta ei voida varmistua, aiheutuu työntekijän omasta laitteesta tietoturvariskejä organisaation verkolle ja tietojärjestelmille.[8]s.64 Henkilökohtaisen laitteen käyttö vaikeuttaa organisaation helpdeskin toimintaa. Ongelmatapauksissa tietotekninen tuki ei pysty ratkaisemaan työntekijöiden laitekohtaisia ongelmia organisaation yhteisten, vakioitujen päätelaitteiden puutuessa. Tietoteknisiä haasteita ratkottaessa tukipalvelun ja työntekijän työaikaa haaskaantuu. Vakioiduille laitteille laaditut yhteiset ohjeet ongelmatapauksiin eivät ole valideja omia laitteita käytettäessä.[8]s.66 Haittaohjelman saastuttaman laitteen havaitseminen ja kirjautumisen esto on keskeinen haaste tietoturvallisuuteen liittyen. Mikäli saastunut päätelaite ei ole hallinnassa ja sen liittymistä organisaation verkkoon ei estetä, haittaohjelman leviäminen verkkoon on todennäköisempää.[8]s.67

BYOD-laitteiden katoamis- ja varkaustapauksissa organisaatiot voivat hallita työntekijöiden mobiililaitteita niiden hallintaan suunnitellulla MDM- eli Mobile Device Management-ohjelmistolla, joka seuraa työntekijän laitteen liikennöintiä ja datan käyttöä tietoverkoissa. Seuraamalla liikennöintiä voidaan ratkaista eteen tulevia ongelmia. MDM-ohjelmistolla BYOD-laite voidaan jäljittää tai organisaation kannalta tärkeän tiedon poistaminen suorittaa etäyhteydellä. MDM-ohjelmiston rinnalla hallintaan voidaan käyttää MAM- eli Mobile Application Management-ohjelmistoa, jolla organisaatio voi rajoittaa omalle toiminnalleen haitallisten sovellusten asentamisen käyttöjärjestelmän sovelluskaupasta.[42]s.10 IT-alan ammattilaiset osaavat parhaiten neuvoa organisaatiota automaattisten hallintatyökalujen käytössä ja suositella tarvittavia korvaavia hallintatoimia asianmukaisen valvonnan varmistamiseksi. BYOD-laite on tunnistettava luotettavaksi, koska vain luotettavalle laitteelle voidaan sallia pääsy organisaation tietoverkkoihin. Älypuhelimen luotettavuus voidaan varmistaa esimerkiksi sen IMEI-koodilla (international mobile equipment identity), tässä tapauksessa tietojen rekisteröinti ja koodien muutokset saattavat aiheuttaa lisätyötä ja sitä kautta kustannuksia.

Työtekijän kannalta ongelmalliseksi voi muodostua henkilökohtaisen päätelaitteen ylläpitokustannukset. Maksaako työnantaja, vaiko työntekijä kustannukset itse, kun työntekijän omaan laitteeseen tarvitaan esimerkiksi tietoturvakokonaisuuksia tai lisenssejä, jotta laite täyttää työnantajan vaatimukset.[8]s.66 Ylläpitokustannusten keskittyessä täysin käyttäjälle itselleen, on olemassa mahdollisuus, että virustorjunnan ylläpitoon ei satsata riittäväsi sen maksullisuuden vuoksi. Työn tekemisen näkökulmasta työntekijän yhteys ympäröivään maailmaan sosiaalisen median sovellusten kautta voi kääntyä myös ongelmaksi. Työhön ei sitouduta sen vaatimalla vakavuudella sosiaalisen median ollessa jatkuvasti työntekijän käsillä.[7]s.2

Oman päätelaitteen kadotessa, huolimattomuudesta tai varkaudesta johtuen, organisaation tuotto sekä tehokkuus laskevat, kunnes työntekijä hankkii tilalle uuden päätelaitteen.[35]
Organisaation näkökulmasta se ei ole yhtä suuri ongelma kuin tiedon päätyminen vääriin käsiin. Työnantajalla tulisi olla kyky laitteen etätyhjentämiseen, mikäli se katoaa tai joutuu vääriin käsiin. Etätyhjennyksen yhteydessä myös työntekijän henkilökohtaisia tiedostoja saatetaan menettää. Organisaatoille haitallisia toimia laitteen joutuessa ulkopuolisen käsiin ovat organisaation tietojen muokkaus päätelaitteella, tietojen lähettäminen eteenpäin tai yritys hallita muita organisaatioon liittyviä laitteita. Työnantajalle ei usein suoda mahdollisuutta oman laitteen etähallinnalle, mikä on huono asia organisaation kannalta.[8]s.67 Vihamielinen taho voi saada hallussaan olevasta BYOD-laitteesta kaikki sille tallennetut tiedot ja tiedostot sekä mahdollisuuden kirjautua laitteella käytettyihin verkkopalveluihin, mikäli työntekijä on tallentanut käyttäjätunnuksen ja salasanan päätelaitteelle.

Tietojen, joita organisaatiot käsittelevät rutiininomaisesti, siirtyminen organisaation ulkopuolelle henkilökohtaiseen päätelaitteeseen aiheuttaa riskejä. BYOD-ympäristössä työntekijät saattavat usein käyttää omia keinojaan tiedostojen lataamiseen ja säilyttämiseen, jotka ovat organisaation tietoturvallisuusohjeiden vastaisia. Organisaatio saattaa esimerkiksi ohjeistaa, että mobiililaitteeseen ladatut tiedostot olisi poistettava asiaankuuluvan kokouksen jälkeen. Työntekijä ei välttämättä kuitenkaan toimi ohjeistuksen mukaisesti. Tiedostosiirron ja pilvipalveluiden turvaaminen on oltava määritelty ja organisaation hallinnassa.[35]

Hyödyt riippuvat näkökulmasta niin kuin Voltti tutkimuksessaan toteaa.[12]s.22 Toisaalta vaikka IT-kustannukset laskevat, niin kokonaiskustannukset eivät todennäköisesti laske yhtä paljoa tai mahdollisesti lainkaan, sillä työntekijöiden käyttämä aika laitteidensa ongelmien ratkaisemiseksi on todennäköisesti pois muusta työajasta. Kokonaiskustannusten voisi jopa epäillä kasvavan, kun ihmiset, jotka eivät ole erikoistuneet IT-ongelmien ratkaisemiseen, käyttävät työaikaansa siihen, jolloin ongelmien ratkaisu ei todennäköisesti ole yhtä tehokasta kuin siihen keskittyneellä henkilöstöllä mahdollisesti olisi. Citrixin kohdalla heidän ilmoittamiaan lukuja tulee arvioida hyvin kriittisesti myös siksi, että he tarjoavat itse teknisiä ratkaisuja BYOD-käytännön osaksi, ja näin ollen heidän liiketoimintansa hyötyy hyvinkin suoraan kasvavasta BYOD-trendistä. [12]s.22

Harriksen mukaan ihmiset eivät mobiililaitteita käyttäessään ole yhtä valveutuneita kuin perinteisten tietokoneiden kanssa. Virustorjuntaohjelmistojen käyttö on vähäistä, koska mobiililaitetta ei nähdä samanlaisena riskinä kuin PC:tä. Käyttäjät hyödyntävät mobiililaitteiden sykronointimahdollisuuksia muiden päätelaitteiden ja palveluiden, kuten sähköpostin ja pilvipalveluiden kanssa. Synkronoituessaan virustorjunnalta suojaamaton mobiililaite altistaa muut päätelaitteet ja palvelut samoille uhille. [19]s.736 BYOD-laitteen tiedostot, kuten valokuvat ja muu materiaali varmuuskopioidaan usein laitevalmistajan pilvipalveluun tiedon säilymisen ja mobiililaitteen rajallisen tallennustilan takia. Tiedon ollessa organisaation omaisuutta, vuotaa BYOD-laite sen ulkopuoliselle taholle, vaikka kyse onkin tavallisesta pilvipalvelusta. Harris toteaa mobiililaitteiden olevan potentiaalinen uhka organisaatiolle, mikäli niiden muodostamaa riskiä ei ole tiedostettu.[19] s.736

Organisaation johdolle BYOD aiheuttaa varmasti ylimääräistä päänvaivaa. Ulkopuolisen laitteen, jolla on voitu käsitellä millaisia tietoja tai selattu mitä tahansa sisältöä liittyy yhtäkkiä organisaation verkkoon käsitellen sen tietoja. Helpoin vaihtoehto johdolle olisi tietenkin omien päätelaitteiden totaalinen kieltäminen, mutta tällöin väärinkäytösten riski voi kasvaa. Ongelmana on, että työntekijät käyttävät omia päätelaitteitaan joka tapauksessa, vaikka organisaation politiikka kieltäisi sen.[43]s.31 Organisaation on huomioitava se omassa suojauksessaan ja valvonnassaan, mikäli näin ei ole jo toiminut. Toimivin ratkaisu voisi olla BYOD-laitteille niin sanottujen kevyiden asioiden hallinta, jotka eivät ole arkaluontoisia.

3.6. BYOD-ohjeistus

BYODin tuomiin tietoturvariskeihin organisaatio pystyy varautumaan ajantasaisella riskien arvioinnilla ja hallinnalla. Organisaation tiedostaessa BYOD-toimintatavan tuomat riskit kykenee se laatimaan tarkat ohjeistukset ja kouluttamaan omien laitteiden tietoturvallisen käytön sen työntekijöille. BYOD-laitteen käyttö ei lisää ainoastaan tietoverkkojen altistumista haitta-ohjelmille vaan työntekijöiden tulee ymmärtää omat vastuunsa tiedon hallinnasta ja sen omistajuudesta. Annettavaa koulutusta sekä BYOD-ohjeistuksia tulee katselmoida säännöllisin väliajoin.[33] s.21-23

Harriksen mukaan organisaation tulisi huomioida mobiililaitteiden osalta seuraavat kokonaisuudet:

- Organisaation tietoa voivat käsitellä vain keskitetysti hallittavat päätelaitteet
- Laitteen käyttäjäprofiilit on salattava ilman mahdollisuutta kyseisten asetuksien muuttamiseen käyttäjän toimesta
- Tiedon salaaminen, automaattiset uloskirjautumiset ja salasana-kyselyt, käyttäjän todentaminen sekä päätelaitteen etätyhjennys oltava käytössä
- Bluetooth-toiminnallisuudet on estettävä
- Vain organisaation sallimien sovellusten asentaminen on mahdollista
- Kameran käyttöä on valvottava
- Sosiaalisen median käyttö on estettävä
- Organisaation tietoturvapolitiikan tulee koskea myös mobiililaitteita
- IEEE 802.1X-standardia on noudatettava [19] s.737

IEEE 802.1X on WLAN- ja Ethernet-verkoissa käytettävä standardi, jonka tarkoituksena on estää luvattomien laitteiden liikenne lähiverkkoon liityntäpisteen eli niin sanotun portin kautta.[44] s.428–429 Edellä mainittujen rajoitteiden ja huomioiden valvominen organisaatiossa saattaa muodostua haastavaksi. Seurauksena voi organisaatioon voi syntyä kulttuuri, jossa BYOD-laitteen käyttö ei ole mahdollista. Esimerkiksi sosiaalisten medioiden käyttö on yleistä varsinkin henkilökohtaisilla päätelaitteilla ja mikäli niitä käytetään BYOD-tarkoituksessa voi sovellusten rajoittaminen muuttua haastavaksi.

Andersson ja Koivisto näkevät kolme tapaa yhdistää oma laite vapaa-aikaan ja työntekoon. Parhaimmaksi vaihtoehdoksi he kokevat sen, että organisaatio ostaa työntekijöilleen laitteet ja näin omistaa ne kokonaisuudessaan. Tässä tapauksessa ei puhuta varsinaisesti BYOD-toimintatavasta vaan organisaation laitteen käytön laajentamisesta. Laitteiden käyttö on kuitenkin sallittua myös vapaa-aikana. Toimintatapana se mahdollistaa parhaiten laitteen etäkäytön ja päivittämisen. Toisena, haastavampana vaihtoehtona Andersson ja Koivisto kokevat sen, että työntekijä käyttää itsekustantamaansa laitetta työntekoon, kuitenkin niin, että organisaatio on taloudellisesti tukenut laitteen hankinnassa ja kuukausittaisissa käyttökustannuksissa. Käyttökustannukset pitäisivät sisällään laitteelle hankittavat sovellukset, kuten virustorjunnan ja niiden ajantasaiset päivitykset. Kolmantena vaihtoehtona he näkevät tavan, jossa työntekijä käyttää omaa laitettaan ilman rahallista tukea. Tämä tapa luo ristiriitaisuuksia päivitys ja ylläpitokustannuksissa, kun organisaatio vaatii laitteelta tiettyä tietoturvatasoa. Järkeväksi nähdäänkin käyttöoikeuksilla rajoittaminen vain osaan organisaation tiedoista. Viimeisin vaihtoehto on Anderssonin ja Koiviston mukaan käytössä ja onnistuu tänä päivänä riittävän hyvin.[8]s.68

Organisaation BYOD-strategiaan kuuluu keskeisesti, että työntekijät hyväksyvät ehdot ja tietoturvan vakavista laiminlyönneistä asetetaan mahdollisia rangaistuksia niiden sattuessa. Tietoturvan laiminlyöntien sattuessa IT-ala voi vahvistaa, että työntekijät ovat allekirjoittaneet käyttäjän hyväksyntäasiakirjat ja he ovat tietoisia yksityisyydensuojasta, mukaan lukien hallintaprosessista henkilötietojen poistamisesta kadonneista tai varastetuista laitteista.[35] Organisaation BYOD-infrastruktuurista on suoritettava asianmukainen tarkastelu, jonka perusteella siinä ilmenevät liikkuvuusongelmat saadaan paikannettua. Niin sanotussa BYOD-auditoinnissa selvitetään omien päätelaitteiden käytön tämänhetkinen tila suhteessa tavoitetilaan.[35] Auditoinnin suorittavat tietoturva-asiantuntijat ovat tärkeässä roolissa BYOD-käyttöönotossa tarjoamalla johdolle itsenäisen ja teknisesti järkevän arvioinnin ongelmista, joita omien päätelaitteiden käyttö lisää.[35] Lisäksi he voivat vakuuttaa, että organisaatio on

käsitellyt uusia liiketoimintaongelmia, jotka johtuvat työntekijöiden, sopimuskumppaneiden ja vierailijoiden yhdistämisestä yritysjärjestelmiin henkilökohtaisten laitteiden kautta.[35]

BYOD-laitteiden hallinnan ja seurannan avulla organisaatiot voivat valvoa hallinta- ja organisaatio-odotuksia, deaktivoida sääntöjä noudattamattomia käyttäjiä. Hallinta ja seuranta antavat organisaatiolle todisteita mahdollisiin rangaistuksiin. Rankaiseminen ei tietoturvallisuuden ylläpitämiseksi ei ole kuitenkaan paras tapa, koska mikäli ilmapiiri ei ole avoin ja kannustava, voi työntekijä jättää kertomatta hallinnan ulkopuolella tapahtuneet tietoturvalaiminlyönnit rangaistuksen pelossa. Organisaation johdon tulisi saada riittävä valvonnan taso BYOD-ympäristössä. Automaattiset valvontatyökalut hälyttävät organisaatiota sääntörikkeen sattuessa ja antavat samanaikaisesti välittömän palautteen työntekijälle omasta toiminnasta. Tavoiteltavassa loppuasetelmassa työntekijä muuttaa toimintatapaansa organisaation haluamaan tietoturvalliseen suuntaan.

Valtiovarainministeriön julkaisemassa VAHTI 5/2013 Päätelaitteiden tietoturvaohjeessa suositellaan BYOD-laitteiden käyttäjiltä allekirjoitettavaa suostumus-lomaketta, jotta organisaation ja käyttäjän vastuut sekä oikeudet ovat selvät, ja kaikkien osapuolten tiedossa. VAHTI 5/2013-ohjeen esimerkki suostumus-lomake sisältää seuraavia asiakokonaisuuksia:

- Päätelaitteella sallittavien tietojen, palveluiden ja tietojärjestelmien käyttö ja tiedonsiirto
- Päätelaitteen katoamisesta seuraavat toimenpiteet ja mahdollinen etätyhjennys esimerkiksi MDM-ohjelmistolla
- Päätelaitteen poistaminen sallittujen laitteiden listalta
- Päätelaitteen tietojen varmuuskopiointi
- Ohjelmien ja ohjelmistopäivitysten asentaminen päätelaitteelle
- Organisaation lisenssien mahdollinen hyödyntäminen BYOD-laitteella
- Ohjelmien ostaminen ja organisaation luottokorttitietojen käyttö
- Päätelaitteen haittaohjelmasuojaus
- Päätelaitteen käyttäjänhallinta ja tunnistaminen
- Päätelaitteen automaattilukitus ja käytettävät suojauskoodit
- BYOD-laitteen käyttö ulkomailla
- Pilvipalveluiden ja sosiaalisen median käyttö (hallinta-, valvonta- ja tukipalvelut sekä mahdolliset laite- tai ohjelmistovalmistajien pilvi-, tunnistus- ja tallennuspalvelut).[21]s.62

4. BYOD-LAITTEIDEN KÄYTTÖJÄRJESTELMIEN TIETOTURVA-VERTAILU

4.1. Käyttöjärjestelmän määritelmä

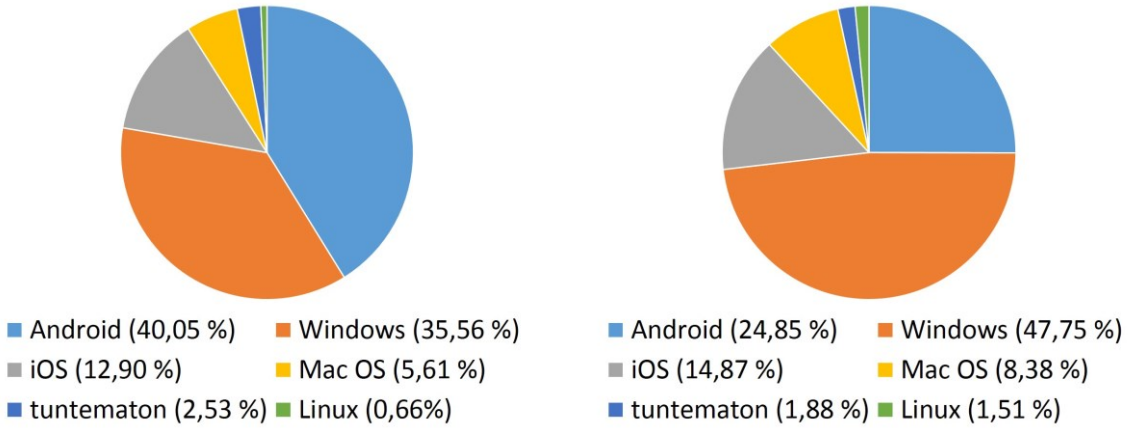
Käyttöjärjestelmä käsitteenä on erotettava loppukäyttäjälle näkyvästä käyttöliittymästä. Käyttöliittymä saatetaan virheellisesti mieltää varsinaiseksi käyttöjärjestelmäksi, vaikka kyseessä on laajempi kokonaisuus.[28]s.11 Päätelaitteen käyttöjärjestelmän tehtävä on liittää laitteisto ja sen sovellukset toimivaksi kokonaisuudeksi, jolla käyttäjä hallitsee päätelaitteensa sisältöä, oli kyse sitten kannettavasta tietokoneesta, tabletista tai älypuhelimesta.[45]s.13 Useiden ohjelmien ja prosessien ollessa samanaikaisesti käytössä, käyttöjärjestelmä jakaa laitteiston resurssit taloudellisimmalla tavalla maksimoiden käytössä olevan suorituskyvyn. Tämä näkyy päätelaitteen käyttäjälle sovellusten nopeana avautumisena sekä käyttöliittymän toiminnan yleisenä sujuvuutena.[28]s.12

Markkinoilla on BYOD-laitteisiin useita eri käyttöjärjestelmiä. Ne eroavat ulkoasultaan, ominaisuuksiltaan, toimintatavoiltaan sekä tietoturvaltaan toisistaan. Käyttöjärjestelmiä on tutkittu useiden tahojen, organisaatioiden ja puolueettomien asiantuntijoiden toimesta. Käyttöjärjestelmissä ilmenevistä haavoittuvuuksista uutisoidaan usein laajasti eri medioissa, jolloin käyttäjien valveutuneisuus käyttöjärjestelmien tietoturvahaavoittuvuuksista olisi ainakin teoriassa mahdollista. Suomessa viimeisimmistä käyttöjärjestelmien haavoittuvuuksista uutisoi tietoturvayritysten ohessa Viestintävirasto.[46] Haavoittuvuuksien ilmetessä käyttöjärjestelmää ylläpitävä yritys ryhtyy toimenpiteisiin riskien poistamiseksi tuottamalla haavoittuvuudet korjaavan päivityspaketin. Automaattisten päivitysten ollessa valittuna päätelaitteen asetuksissa, poistuvat käyttöjärjestelmän sekä sovelluksien haavoittuvuudet päivityspakettien asentumisen myötä.[47][48][49] Massiivisia toimenpiteitä käyttöjärjestelmän tietoturvallisuuteen ei käyttäjältä itseltään vaadita, kun automaattiset päivitykset päätelaitteella on valittuna asetuksista. Viestintäviraston teettämän tutkimuksen mukaan 98 prosenttia 25–34 vuotiaista suomalaisista päivittää päätelaitteensa aktiivisesti, mutta iäkkäämmät käyttäjät eivät ole yhtä aktiivisia. Tutkimuksen mukaan 75 prosenttia vastaajista, jotka pitivät päivityksiä tarpeettomina, olivat yli 50-vuotiaita.[50]

Käyttöjärjestelmistä voidaan puhua avoimina tai suljettuina, riippuen siitä minkälaiseen lähdekoodiin ne perustuvat. Yksinkertaistettuna avoimen järjestelmän lähdekoodi on kaikkien nähtävillä ja suljetun vain tuotteen valmistajalla. Hyökkääjät etsivät haavoittuvuuksia kummankin tyylistä käyttöjärjestelmistä, joten kokonaisuuden on oltava turvallinen. Tästä aiheesta keskusteltaessa mielipiteet jakautuvat avoimen järjestelmän puolesta ja vastaan. Avoimuuden hyötyjä ovat järjestelmien välinen toimivuus samoissa verkoissa. Avointen järjestelmien taustalla työskentelee suuri joukko vapaaehtoisia eri teknologian aloilta pyrkimyksenä tietoturvallisemman käyttöjärjestelmän luominen. Periaatteessa koodi on kaikkien nähtävillä, joten haavoittuvuuksia kyetään löytämään ja niitä pystytään korjaamaan, mutta myös hyödyntämään vihamielisissä tarkoituksissa. Avoimia käyttöjärjestelmiä ovat Linuxiin pohjautuvat Debian, Ubuntu ja Android.[51]s.6 [19] s.408 Suljettu käyttöjärjestelmän tuottaja ei luovuta lähdekoodiaan ulkopuoliselle eli pitää kokonaisuuden rakenteen itsellään. Suljettu järjestelmä on suunniteltu kommunikoimaan vain tiettyjen sovellusten kanssa. Eristyneisyys on myös suljetun järjestelmän turvallisuuden perusta.[19] s.408 Suljettuja käyttöjärjestelmiä ovat Windows-käyttöjärjestelmät. Applen iOS ja Mac OS ovat niin sanotusti avoimen ja suljetun välistä, koska ne perustuvat avoimeen Darwin-ytimeen ollen kuitenkin Applen tuotteina vahvasti kontrolloituja, jolloin käyttäjällä on rajallisemmat mahdollisuudet käyttöjärjestelmän muokkaamiseen sekä sovellusten asentamiseen.[29]s.44 [14]

4.2. Yleisimmät käyttöjärjestelmät

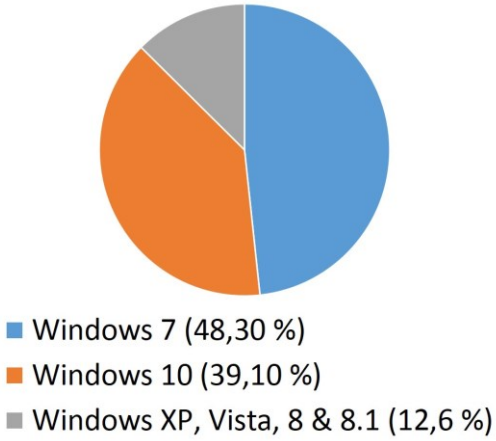
Yleisimmät käyttöjärjestelmä-perheet maailmassa ovat Android, Windows, iOS, Mac OS sekä Linux.[52] Tarkasteltaessa käyttöjärjestelmien markkinaosuuksia kaikilla päätelaitteilla, jako on seuraavien kaavioiden osoittama. Suomessa yleisin käyttöjärjestelmä on Windows Androidin ollessa toisella sijalla. Syynä tähän on maailmalla tapahtuva älypuhelinten voimakas yleistyminen ja PC-koneiden suosion hiipuminen. Ilmiön voidaan odottaa tapahtuvan lähivuosina myös Suomessa.



Kuva 6. Käyttöjärjestelmien markkinaosuudet tammikuussa 2018. Vasemmalla maailma [52], oikealla Suomi [53]

Etenkin Suomessa laajemmassa käytössä ollut Microsoftin tuottama WindowsPhone-käyttöjärjestelmän tuotto ja ylläpito ovat Microsoftin toimesta päättyneet vuonna 2017.[54] Tämä tarkoittaa sitä käyttävien laitteiden ohjelmisto- sekä tietoturvapäivitysten päättymistä. Riskit kyseisillä laitteille siis lisääntyvät, koska mahdollisia haavoittuvuuksia ei enää korjata. Edellä mainituista syistä BYOD-laitteessa WindowsPhone-käyttöjärjestelmän voidaan olettaa olevan tietoturvauhka organisaatiolle, jossa sitä käytetään. WindowsPhone-käyttöjärjestelmää ei vertailla tutkielmassa muihin käyttöjärjestelmiin. Seuraavaksi esitellään yleisimmät käyttöjärjestelmät Suomen markkinaosuuteen perustuvassa järjestyksessä aloittaen yleisimmästä.

Windows on Microsoftin kehittämä käyttöjärjestelmä PC:lle eli henkilökohtaisille tietokoneille, jonka ensimmäinen MS-DOSiin perustuva versio tuli markkinoille vuonna 1985. Windows-käyttöjärjestelmäperhe kokonaisuutena on maailmanlaajuisesti yleisin käyttöjärjestelmä PC-puolella.[55]



Kuva 7: Windows markkinaosuudet maailmassa tammikuussa 2018 [56]

Tarkastellessa Windowsin versioiden markkinaosuuksia, jotka kuvassa 7 on nähtävissä, että Windows 7 ja Windows 10 versiot ovat eniten käytössä olevia käyttöjärjestelmän versioita tammikuussa 2018. Näiden versioiden suosio voi selittyä niiden stabiiliudella. Lisäksi version 8 ja 8.1 Windowseista monet sisälsivät option päivitykselle uusimpaan 10-versioon. Windows on päättänyt tukensa 7-versiolle 13.1.2015, jonka jälkeen käyttäjien on ollut mahdollista lunastaa jatkoaikaa päivityksille Extended-tukijakson muodossa, joka päättyy 14.1.2020. Tämänhetkisten Windows 10-versioiden elinkaari päättyy 2018–2019 kuluessa. Käyttöjärjestelmää tuetaan tietoturvapäivityksillä sen elinkaaren ajan, jonka jälkeen se altistuu helpommin tietoturvauhille. [57]

Android on Googlen omistama ja tuottama mobiilialustoilla toimiva käyttöjärjestelmä, joka pohjautuu Linuxin version 2.6 avoimeen lähdekoodiin, johon perustuvat muun muassa käyttöjärjestelmän turvallisuus, muistinhallinta, prosessien hallinta sekä verkkotoiminnallisuudet.[58] Androidin toiminta perustuu useiden prosessien samanaikaiseen toimintaan. Jokainen käytettävä sovellus ja käyttöjärjestelmän osa käyttää omaa prosessiaan. Käyttöjärjestelmän turvallisuus luodaan Linux-ytimen kautta sovellusten ja järjestelmän prosessitasolla, käyttäjä- ja ryhmätunnusten avulla. Suoritettavat turvallisuustoimenpiteet ajetaan niin kutsutun lupamekanismin läpi, joka pakottaa tietyn prosessin suorittamat erityistoimet ja URI-käyttöoikeudet tietyille tietolähteille tapahtuvan tilapäisen pääsyn myöntämiseksi.

iOS on Apple Inc. tuottama mobiilikäyttöjärjestelmä, jota käytetään iPhone-älypuhelimilla ja iPad-tableteilla. Mobiilikäyttöjärjestelmä on tehty yhteensopivaksi MacOS-käyttöjärjestelmän ja Applen muiden palveluiden kanssa. iOS-käyttöjärjestelmän laitteet yhteensovittavat ohjelmistot, laitteiston ja palvelut luoden turvallisen sekä käyttäjäystävällisen kokonaisuuden. iOS suojaa itse laitteen ja sen käyttämän datan lisäksi koko ekosysteemin sisältäen kaiken käyttäjän toiminnan laitetasolla ja internetissä. [59]s.4

MacOS on Apple Inc yhtiön valmistamien Mac-tietokoneiden käyttöjärjestelmä. MacOs on helppokäyttöinen ja käyttäjäystävällinen käyttöjärjestelmä, joka hyödyntää Applen hallinnoimaa iCloud-pilvipalvelua. iCloudin avulla käyttäjän tiedostot, kuten valokuvat ja tiedostot on tallennettavissa pilveen, jolloin niiden käyttö on mahdollista kaikilla käyttäjän MacOS ja iOS-laitteilla, kuten iPhone-älypuhelimella. Applen mukaan MacOS on kokonaisuudessaan alhaalta ylös asti tehty käyttäjän yksityisyyttä ja tietoturvallista käyttöä ajatellen. Käyttöjärjestelmää markkinoidaan sen soveltuvuudella luoville aloille, kuten kuvien ja videoiden käsittelyyn, tuotannollisiin tehtäviin työssä sekä sovellusten mahdollistamaan helppoon kommunikointiin. Applen iOS ja Mac OS käyttävät useita samoja sovelluksia ja ovat rakenteeltaan samankaltaisia, jolloin haittaohjelmien siirtyminen niiden välillä on todennäköistä. [60]

Linux on suomalaisen Linus Thorvaldsin työryhmineen kehittämä ja vapaaehtoisten ylläpitämä UNIX-käyttöjärjestelmään pohjautuva käyttöjärjestelmä, jonka ensimmäinen versio käyttöönotettiin syyskuussa 1991. Linux perustuu avoimeen lähdekoodiin ja sitä käytetään useilla eri päätelaitealustoilla niin tietokoneilla kuin älypuhelimillakin.[61] Linuxiin perustuvia käyttöjärjestelmäversioista puhuttaessa käytetään käsitettä jakelu tai jakelupaketti.[62] s.15 Tunnettuja jakeluita ovat muun muassa Debian sekä Ubuntu.[63][64] Linux jakelut ovat käyttäjilleen täysin ilmaisia tietoturvapäivityksineen ja perusohjelmistoineen.[65] Avoin lähdekoodi mahdollistaa käyttöjärjestelmän toiminnan todentamisen. Linux on pohjimmiltaan turvallinen käyttöjärjestelmäkokonaisuus, joka vapaaehtoisten ylläpitämänä kehittyy jatkuvasti. Linuxin heikkoudet ovat sen vaativuudessa käyttäjälle. Käyttäjältä vaaditaan työtä enemmän kuin muissa PC-käyttöjärjestelmissä eikä sovelluksia ole saatavilla samassa määrin kuin Windowssille ja Mac OS:lle.[62]s.27

Seuraavaksi yleisimpiä käyttöjärjestelmiä vertaillaan tietoturvan osalta keskenään niistä löydettyjen haavoittuvuuksien sekä koventamisohjeiden perusteella. Käyttöjärjestelmien vertailun jälkeen kerrotaan omissa alaluvuissaan syvemmin PC- ja mobiilikäyttöjärjestelmien lähivuosina havaittuja haavoittuvuuksista sekä niiden korjaustoimenpiteitä. Viimeisessä alaluvussa tehdään johtopäätöksiä käyttöjärjestelmien tietoturvasta.

4.3. Käyttöjärjestelmien tietoturvavertailu

Käyttöjärjestelmät ovat muuttuneet yksinkertaisemmista järjestelmistä monimutkaisemmiksi kokonaisuuksiksi, jolloin niiden suojauksen tärkeys on kasvanut.[29]s.601 Silberschatz et al. mukaan käyttöjärjestelmien rikkomukset voidaan jakaa tahallisiin ja tahattomiin. Järjestelmien suojaus usein rakentuukin tahattomien rikkomusten suojaamiseen.[29]s.634

Käyttöjärjestelmien tietoturvaa vertaillaan The National Institute of Standards and Technology (NIST) NVD-tietokantaan (National Vulnerability Database) pohjautuvia CVSS-pisteytystä viimeisen kolmen vuoden ajalta. NIST on Yhdysvaltain kauppaministeriöön kuuluva organisaatio, jonka tekemiä mittauksia hyödynnetään monipuolisesti eri teollisuuden aloilla.[66] NVD-tietokannan aineistoon perustuvaa statistiikkaa tutkimukseen kerättiin cvedetails.com sivustolta, joka kokoaa raportoidut haavoittuvuudet tietokantaansa. Lisäksi BYOD-laitteiden käyttöjärjestelmien vertailussa hyödynnetään Center of Internet Securityn eli CIS:n tuottamia käyttöjärjestelmien koventamisoppaita. CIS on voittoa tavoittelematon IT-ammattilaisten muodostama organisaatio, joka käyttää resurssejaan tuottaen yksityishenkilöille sekä organisaatioille suojaa kyberuhkia vastaan tuottamalla CIS Control ja CIS Benchmark koventamisohjeita ja oppaita.[67] Koventamisoppaissaan CIS opastaa käyttäjiä käyttöjärjestelmään tehtävistä toimenpiteistä, jotka suorittamalla käyttöjärjestelmälle potentiaaliset tietoturvauhat saadaan minimoitua tai kokonaan poistettua. Tällöin puhutaan niin sanotusta käyttöjärjestelmän koventamisesta. Toimenpiteet vaihtelevat yksinkertaisista asetusten muutoksista monimutkaisempiin konfiguraatioihin. Muutokset voidaan suorittaa osittain käyttäjän itsensä toimesta asetusmuutoksilla tai XML-tiedoston ajamisella päätelaitteelle esimerkiksi organisaation MDM-ratkaisun avulla. Lähestymiskannaksi tietoturvavertailuun käytetään näitä tapoja, jotta aineistot ovat niin sanotusti samat. Android ja iOS ovat mobiililaitteille kehiteltyjä käyttöjärjestelmiä muiden ollessa PC-koneille suunniteltuja. Rakenteellisesti näissä on eroja ja niiden tietoturvallisuus perustuu eri lähtökohtiin. Tarkastellessa käyttöjärjestelmän tunnettuja haavoittuvuuksia saadaan suuntaa antava kuva siitä, minkälaisia eroja kaikkien BYOD-päätelaitteiden käyttöjärjestelmillä on.

Seuraavaksi vertaillaan yleisimpien käyttöjärjestelmien haavoittuvuuksia sekä koventamissuosituksia. Näiden perusteella kyetään luomaan mielikuva käyttöjärjestelmien tietoturvallisuuden tasosta.

4.3.1. Haavoittuvuudet

Common Vulnerability Scoring System eli CVSS on haavoittuvuuksien arviointiin käytettävä yhtenäinen pisteytysjärjestelmä. CVSS perustuu kolmeen pisteytettävään osa-alueeseen:

- Base: kuvaa haavoittuvuuden luontaisia ja perusominaisuuksia, jotka ovat pysyviä suhteessa aikaan ja käyttäjäympäristöön
- Temporal: kuvaa haavoittuvuuden luonteen pysyvyyttä suhteessa aikaan
- Environmental: kuvaa haavoittuvuuden luonnetta suhteessa tiettyyn käyttäjäympäristöön. [68][69]

CVSS-pisteytys jaetaan seuraavasti kuvaamaan kunkin haavoittuvuuden vakavuutta:

- 0 - ei uhkaa
- 0,1 - 3,9 – matala
- 4,0 – 6,9 – keskitaso
- 7,0 – 8,9 – korkea
- 9,0 – 10,0 – kriittinen [69]

Vertailtavien käyttöjärjestelmien osalta tarkastellaan niiden haavoittuvuuksia vuosina 2015 – 2017. Kunkin vuoden aikana raportoidun haavoittuvuus-lukumäärän ohella kerrottu prosenttiluku ilmoittaa, montako prosenttia haavoittuvuuksista on ollut kriittisiä. Lopuksi vuosien 2015 - 2017 raportoitujen haavoittuvuuksien kokonaismäärä, kriittisten prosentuaalinen määrä, sekä tarkasteltujen vuosien haavoittuvuuksien CVSS-pisteytyksien keskiarvo. Lukuarvojen tarkastelussa tärkeää on kriittisten haavoittuvuuksien prosentuaalinen osuus.

Taulukko 1. Käyttöjärjestelmien haavoittuvuudet ja CVSS-pisteytys 2015–2017. [70]

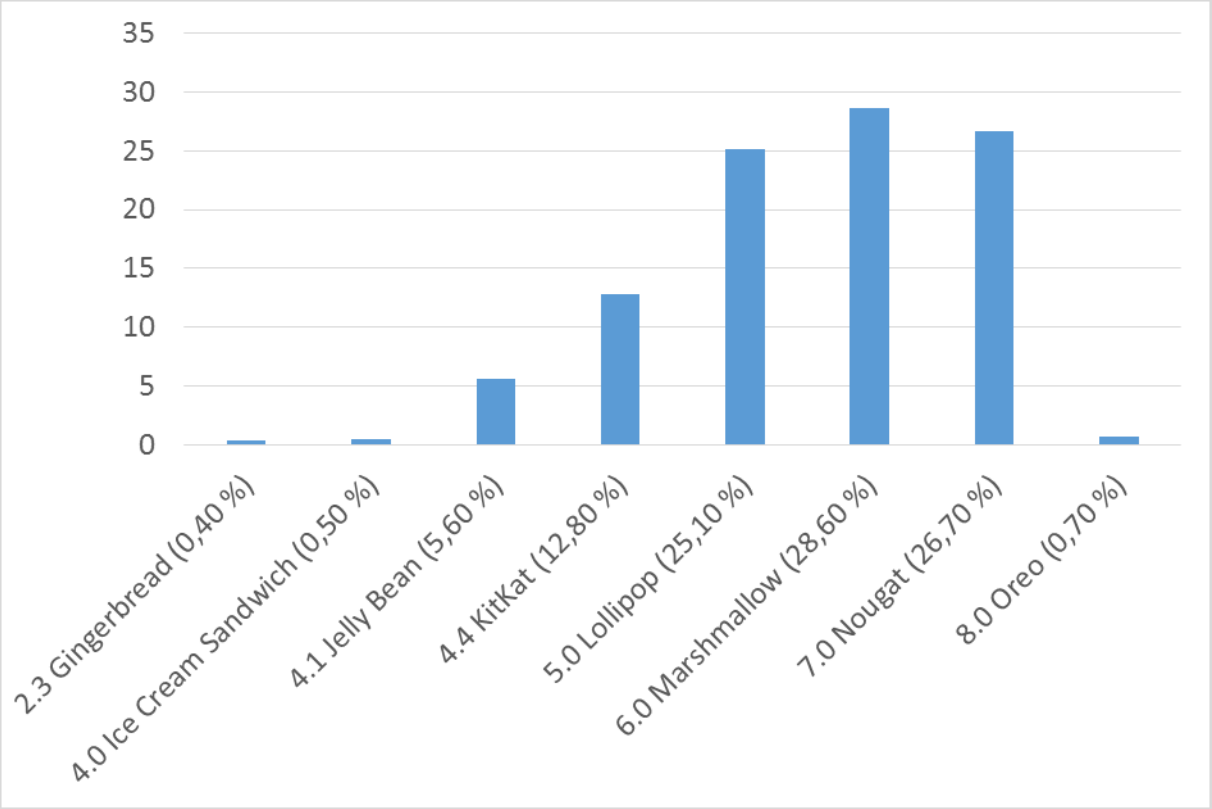
Haavoittuvuudet / kriittiset haavoittuvuudet	Win 7	Win 10	Mac OS X	iOS	Android	Debian Linux	Ubuntu Linux
2015	147 / 33,3%	53 / 28,3%	444 / 16,9 %	387 / 8,3 %	125 / 70,4%	235 / 6,8%	261 / 8,8%
2016	134 / 35,8%	172 / 32,6 %	215 / 37,20%	161 / 32,3 %	523 / 48,6%	327 / 8,3%	279 / 8,2%
2017	229 / 13,5%	268 / 9,0 %	299 / 31,4 %	387 / 15,5 %	842 / 41,1%	230 / 3,0%	84 / 2,4%
Yhteensä	510 / 25,1%	493 / 19,3 %	958 / 26,0 %	935 / 15,4 %	1490 / 46,2%	792 / 6,3%	624 / 7,7%
CVSS Score ka. (2015-2017)	6.6	6.4	7.3	6.8	8.1	6.4	6.3
”CVSS-taso”	keski-taso	keski-taso	korkea	keski-taso	korkea	keski-taso	keski-taso

Annetut pisteytykset perustuvat NVD-tietokantaan, jossa Mac OS-perhettä tarkastellaan yhtenä kokonaisuutena ja Windowsin sekä Linuxin käyttöjärjestelmäversioita erillisinä kokonaisuuksina. Windows 10 virallinen julkaistiin virallisesti heinäkuun lopulla 2015 [55], joka on nähtävissä haavoittuvuuksissa 2015. Tämä on tiedostettava johtopäätöksiä tehdessä. Arvoja analysoidessa ja käyttöjärjestelmiä vertaillessa on huomattavissa eroja näiden välillä. Lisäksi vertailtavissa arvoissa on syytä painottaa kriittisten haavoittuvuuksien prosentuaalista määrää kokonaistuloksen sijaan, koska monet haavoittuvuudet voivat olla pieniä ja suuremman kokonaisuuden kannalta vähemmän merkityksellisiä.

Androidin kohdalla on monta negatiivista huomiota muihin käyttöjärjestelmiin liittyen. Mobiilikäyttöjärjestelmissä on havaittavissa Androidin raportoitujen haavoittuvuuksien lisääntyminen suhteessa Applen iOSiin sekä PC-käyttöjärjestelmiin. Haavoittuvuuksien CVSS-pisteytyksen perusteella Androidin haavoittuvuuksista lähes puolet (46,2 %) ovat kriittisiä, se on vertailtavasta joukosta selkeästi korkein tulos. Nortonin analyytikkojen mukaan syyksi Androidin haavoittuvuuksien paljastumiselle voidaan pitää sen maailmanlaajuisen suosion ja avoimuuden taustalla olevien hyökkäysten suurta lukumäärää. [71]

Avoimena käyttöjärjestelmänä Android sallii käyttäjän lataamaan sovelluksia miltä tahansa toimittajalta. Kuten kotikoneessa, käyttäjän on oltava tietoinen siitä, kuka toimittaa ladattavan ohjelmiston, ja hänen on päätettävä, myöntääkö hän sovellukselle vaaditut ominaisuudet. Tätä päätöstä voidaan saada tietoisesti arvioimaan ohjelmiston kehittäjän luotettavuus ja siitä, mistä ohjelmisto on peräisin.[72]s.24

Androidin haavoittuvuuksien taustalla ovat myös lukuiset käytössä olevat käyttöjärjestelmän versiot sekä laitevalmistajien muutokset alkuperäiseen, puhtaaseen Androidiin. Cambridgen yliopiston tekemän tutkimuksen mukaan Android-käyttöjärjestelmän laitteita päivitetään myyntihetkestä alkaen 12–24 kuukautta, keskiarvona 1,26 kertaa vuodessa. Harvoin päivittyvät päätelaitteet ovat pitkiä aikoja alttiina tietoturvauhille. Laitevalmistajien päätelaitteilla on suuria tietoturvaeroja, koska julkaistuja tietoturvapäivityksiä ei jalkauteta suoraan päätelaitteille. Esimerkiksi Googlen tuottamat Nexus-laitteet saavat uusimmat Android-päivitykset muiden tutkimuksessa olleiden laitevalmistajien päätelaitteita nopeammin. Laitevalmistajien viivästykset tietoturvapäivitysten julkaisemisessa altistavat yrityksen tuottamat päätelaitteet tietoturvauhille. [73]s.11



Kuva 8: Käytössä olevien Android-versioiden markkinaosuudet tammikuussa 2018 [74][75]

Tutkimuksessa havaittiin jopa 87,7 prosenttia Android-käyttöjärjestelmän laitteista altistuvan ainakin yhdelle tutkimuksessa olleelle yhdelletoista haavoittuvuudelle. Tutkijat käyttivät arvioidessaan Androidia FUM-pisteytystä, joka koostuu kolmesta osatekijästä:

- f , laitteiden osuus tunnetuista kriittisistä haavoittuvuuksista
- u, laitteiden osuus, jotka on päivitetty viimeisimpään versioon
- m, haavoittuvuuksien osuus, joita laitevalmistaja ei ole vielä korjannut [76]

Kokonaisuudessaan Android sai ekosysteeminä 2,87 pistettä täydestä kymmenestä pisteestä. Googlen Nexus sai 5,17 pistettä ollen tutkimuksen paras yksittäinen päätelaite.[73]s.11

Nykyään Google tarjoaa kuukausittain uusimmat tietoturvapäivitykset niin sanotuille puhtaille ja alkuperäisille Androideille eli Nexus, Pixel sekä HDM Globalin valmistamille Nokia-puhelimille automaattisesti.[77] Muut laitevalmistajat lykkäävät päivityspakettien asentamista syystä tai toisesta, jolloin vanhan version puutteet ovat kyseisillä laitteilla. [78]

Päivityksiä on saatavilla vain uusimpiin versioihin ja vanhemmat Android versiot jäävät ilman tärkeitä tietoturvaa parantavia päivityksiä. Nortonin mukaan valtaosasta Androidin tietoturvaheikkouksista päästäisiin, jos kaikki päätelaitteet olisivat käyttöjärjestelmäpäivitysten

piirissä. Google ei enää tue 5.0 Lollipoppia vanhempia käyttöjärjestelmäversioita eli markkina osuuksia tarkastella 19,3 prosenttia käytössä olevista Android-päätelaitteista on täysin vailla uusia tietoturvapäivityksiä. Vastaavaa ongelmaa ei ole iOSin kohdalla, koska Applen politiikkaan kuuluu käyttöjärjestelmän ajantasaisuuden ylläpito laajoilla päivityspaketeilla.[71] Androidin Google Play-sovelluskauppa mahdollistaa avoimemman sovellusten lisäämisen, mahdollistaen kenen tahansa tuottaa päätelaitteelle ladattavia sovelluksia. Vahvan kontrollin puuttuessa vihamielisten sovellusten leviäminen on mahdollista. Googlen julkaiseman turvallisuusraportin mukaan Android-laitteet, joiden sovellukset on ladattu Googlen omasta Play-sovelluskaupasta altistuvat yhdeksän kertaa vähemmän haittaohjelmille kuin kolmansilta osapuolien sovelluskaupoista. Raportin mukaan haittaohjelman lataamisen todennäköisyys Google Playn kautta laski 50 prosenttia vuoden 2017 aikana, todennäköisyyden ollessa 0.02 prosenttiyksikköä.[51]s.5

Vertailussa vähiten kriittisiä haavoittuvuuksia sisältävät Linuxin versiot Debian ja Ubuntu. Mac OS X haavoittuvuuksien määrä on laskenut lähivuosina, mutta kriittisten haavoittuvuuksien osuus on noin kolmanneksessa. Windows 7 ja 10 haavoittuvuudet ovat nousussa, johon on muutamia todennäköisiä syitä. Ensiksi Windows 7-version päivitystuki on päättynyt alkuvuodesta 2015, Extended-tuen jatkuessa vuoteen 2020. Haavoittuvuuksista kärsivät tukemattomat versiot eivät korjaannu ilman päivityspaketteja. Toiseksi Windowsin haavoittuneisuuteen voidaan yleisesti pitää syynä sen suurempaa käyttöprosenttia maailmanlaajuisesti. Kolmanneksi haavoittuvuuksien lisääntymiseen Windows-alustalla on syynä Windows 10 markkinaosuuden kasvu, jolloin sen kiinnostus hyökkääjien keskuudessa on varmasti lisääntynyt.

4.3.2. Suositeltavat kovennukset

Vertaillessa yleisimpien BYOD-laitteiden käyttöjärjestelmien uusimmille versioille tuotettuja koventamisohjeiden pituuksia, on havaittavissa osan olevan huomattavasti toisia pitempiä. Toisin sanoen käyttöjärjestelmän koventamisopas on sitä pidempi, mitä enemmän siinä on tietoturvaparannuksia vaativia haavoittuvuuksia. Koventamisohjeessa suositeltavat asetusmuutokset jaotellaan ”scored” ja ”not scored”-suoritteisiin sen perusteella vaikuttaako kyseinen muutos käyttöjärjestelmän lopulliseen CIS Benchmark-pisteytykseen. Alla olevaan taulukkoon on listattu CIS Benchmark-koventamisohjeessa esiintyvien kovennettavien asetusten määrän.

Taulukko 2. Käyttöjärjestelmille suositellut CIS Benchmark-kovennukset.[79][80][81][82][83][84][85]

Käyttöjärjestelmä	Microsoft Windows 7	Microsoft Windows 10 Enterprise	Apple OSX 10.12	Apple iOS 11	Google Android 8.x.x	Debian Linux 8	Ubuntu Linux 16.04 LTS
Scored	389	473	78	57	0	143	188
Not Scored	1	1	33	8	39	43	32
Yhteensä	390	474	111	65	39	186	220

CIS Benchmark-ohjeiden perusteella puhdas Android 8 ja iOS 11 ovat vertailtavien käyttöjärjestelmistä turvallisimmat perustuen CIS:n suosittelemiin kovennuksiin. Perinteisien PC-käyttöjärjestelmien osalta vähiten asetusmuutoksia suositellaan tehtäväksi Applen OS X 10.12:seen. Linux Debian 8 ja Ubuntu 16.04 LTS vaativat määrällisesti lähes yhtä paljon asetusmuutoksia. Eniten asetusmuutoksia CIS:n mukaan tarvitaan Microsoft Windows 10 Enterprise-käyttöjärjestelmässä, jopa kaksi kertaa enemmän kuin toiseksi viimeiseksi tuleva Ubuntu. On pääteltävissä, että taulukon käyttöjärjestelmistä Windows 10 Enterprise on turvattomin, koska se vaatii suuren määrän asetusmuutoksia ollakseen niin sanotusti kovennettu. Seuraavassa alaluvussa käsitellään yleisimpien käyttöjärjestelmien haavoittuvuuksia hyödyntäneitä haittaohjelmia lähivuosilta.

4.3.3. Haavoittuvuuksia hyödyntäneitä haittaohjelmia

Elokuussa 2016 Pegasus-niminen haittaohjelma hyödynsi käyttöjärjestelmästä löytyvää aukkoa iOS 7-versiossa. Pegasus otti haltuunsa päätelaitteen päästen käsiksi salasaoihin, viesteihin, sähköposteihin sekä puhelutietoihin sekä tunnettujen sovellusten, kuten Whatsappin, Skypen ja Gmailin kirjautumistietoihin.[71] Apple paikkasi tietoturva-aukon iOS 9.3.5 käyttöjärjestelmäpäivityksellä. [86] Ennen päivityspaketin jakamista Pegasus-tartuntoja havaittiin myös MacOS puolella OS X 10.10 Yosemite ja OS X 10.11 El Capitan versioissa sekä Safari-verkkoselaimessa. [87]

Australialainen tutkija Mark Dowd havaitsi iOSin ja Mac OS X:n kriittisen haavoittuvuuden Applen langattoman tiedonsiirron protokollassa. Tämä AirDrop-protokollan haavoittuvuus mahdollisti haitallisen tiedoston lähettämisen ja sitä kautta haittaohjelman asentamisen mihin tahansa AirDrop-yhteensopivaan päätelaitteeseen eli käytännössä jokaiseen Applen päätelaitteeseen. Kriittiseksi haavoittuvuuden teki se, että vihamielisessä tarkoituksessa lähetetyn tiedoston vastaanottamista ei tarvinnut hyväksyä. Päätelaite olisi merkinnyt vastaanotetun tie-

doston luotetuksi, jolloin sen edelleen lähettäminen olisi ollut helpompaa. Luotettavana tiedosto ja sen sisältävä ohjelma sai laajat käyttöoikeudet, jolloin sen avulla pääsi käsiksi päätelaitteen yhteystietoihin, sijaintitietoihin ja kameraan. Dowdin havaitseman haavoittuvuuden jälkeen Apple muokkasi AirDropin toimimaan niin sanotussa sandboxissa eli hiekkalaatikossa, jolloin sen pääsyä käyttöjärjestelmän muihin osiin rajoitettiin. [88]s.25

Indianan yliopiston vuonna 2015 julkaisemassa tutkimuksessa havaittiin neljä keskeistä haavoittuvuutta Applen tuotteissa. Niin kutsutulla XARA-hyökkäyksellä (Cross-app Resource Access Attack) Applied tutkijat kykenivät ohittamaan turvakontrollit ja varastamaan arkaluontoista dataa käytetyistä sovelluksista. Tutkijat onnistuivat saamaan käyttäjän tietoja muun muassa seuraavista yleisessä käytössä olevasta sovelluksista:

- iCloud
- Gmail
- Google Drive
- Facebook
- Twitter
- Dropbox
- Instagram
- Whatsapp sekä
- Chrome-selaimen kautta tehtyjä kirjautumisia

XARA-hyökkäyksen lisäksi Indianan yliopiston tutkijat onnistuivat lisäämään haittaohjelman Applen AppStoreen. Yliopiston tutkijat raportoivat havainnoistaan Applelle ja julkaisivat tutkimuksen, kun haavoittuvuudet oli saatu korjattua.[88] s.20–21 Haavoittuvuuksien korjaamisessa kului kuusi kuukautta ja ne paikattiin käyttöjärjestelmän päivityspaketilla. [89]

Tutkimuksessa havaittiin haavoittuvuudet:

- Keychain-salasanan tallennusominaisuudessa
- BID-tunnuksessa
- Prosessien välisen viestinnän salauksessa sekä
- URL-tiedon välityksessä sovellusten välillä

Applen-käyttöjärjestelmissä on suojattu Keychain-ominaisuus, jonka avulla käyttäjä voi tallentaa ja hakea salasanoja eri sovelluksille ja verkkopalveluille. Yksi neljästä tutkimuksen haavoittuvuudesta salli haitallisen sovelluksen luoda etukäteen Keychain-merkinnän toiselle

sovellukselle. Mikäli kohdennettua sovellusta ei oltu asennettu päätelaitteelle, ja käyttäjä asensi sovelluksen myöhemmin, sen tunnisteet tallennettiin haitallisen sovelluksen luomalla Keychain-merkinnällä. Jos kohdistettu sovellus oli asennettu, pystyi haitallinen sovellus poistamaan olemassa olevan Keychain-merkinnän ja luomaan uuden, joka aktivoitui seuraavalla kerralla, kun käyttäjä avasi kohdistetun sovelluksen.[88] s.21

Toinen haavoittuvuus mahdollisti haitallisen sovelluksen pääsyn toisen sovelluksen suojattuihin tietoihin ja varastamaan sovelluksesta tietoja. Jokainen sovellus yksilöidään BID-tunnuksella (Bundle ID).App Store ei salli muiden sovellusten käyttää BID-tunnusta, joka on ollut toisella sovelluksella. Haavoittuvuus esiintyi sovellusten laajennuksissa, joiden BID-tunnusta App Store ei tarkistanut. Haavoittuvuutta hyödyntäen päästiin käsiksi toisen sovelluksen sisältämiin tietoihin.[88] s.21

Kolmas haavoittuvuus oli Mac OS X:n prosessien välisen viestinnän salauksessa, jonka vikoja hyödyntämällä päästiin käsiksi sovellusten käyttämiin salasanoihin ja dataan. Neljäs haavoittuvuus löytyi URL-ohjelmasta, jota sovellukset käyttävät keskinäisen tiedonvälitykseen. Haavoittuvuus olisi mahdollistanut haittaohjelman vastaanottamaan toisen sovelluksen lähettämät tiedot ja koko järjestelmän kaappaamisen.[88] s.21

5. TEEMAHAASTATTELU

5.1. Toteutus

Haastateltavia lähestyttiin Outlook-sähköpostilla ja lähetettyä viestiä seuranneessa keskustelussa sovittiin tarkempi ajankohta ja paikka teemahaastattelulle. Lähtökohtana oli, että haastattelu tehdään asiantuntijoiden kannalta suotuisimmassa ympäristössä, eli heidän omalla työpisteellään tai työhuoneessaan. Teemahaastattelun arvioitu kesto oli noin yksi tunti ja haastattelujen toteutunut kesto vaihteli kahdestakymmenestä minuutista yhteen tuntiin. Haastattelutilanteet pyrittiin järjestämään tutkijan ja yhden haastateltavan välillä, mutta aikataulullisista syistä yhteen teemahaastatteluun osallistui kaksi henkilöä samanaikaisesti. Kahden haastateltavan kanssa käytyä haastattelua ei koettu ongelmalliseksi, ehkä jopa päinvastoin. Haastateltavat tukivat vastauksissaan toisiaan, tuoden esille myös poikkeavia näkemyksiä ja vastauksia.

Teemahaastattelut suoritettiin tammi-helmikuussa 2018. Haastateltavia oli kokonaisuudessaan yhdeksän kappaletta, joista viisi työskentelee puolustusvoimissa ja neljä kyberturvayhtiö Nixu Oyj:ssä, joka tarjoaa asiakkaina toimiville yrityksille ja organisaatioille kyberturvallisuuspalveluita. [90] Puolustusvoimissa työskentelevät toimivat tai ovat toimineet tietohallintoalalla, kyberturvallisuuden tehtävissä tai tutkimustyössä. Heistä yksi toimii sotilastehtävissä ja neljä siviilitehtävissä. Nixu Oyj:n haastateltavien työtehtäviin kuuluu organisaation omasta tietoturvasta vastaaminen, tietoturvasovellusten kehittäminen, ohjelmointi, mobiiliapplikaatioiden ja – laitteiden tietoturva sekä hallinnollinen tietoturva. Teemahaastatteluun osallistuneet löytyvät tutkimuksen liitteestä 1.

Haastattelun aikana käytävä keskustelu äänitettiin tutkijan omistamalle digitaaliselle SONY ICD-BX140 sanelukoneelle. Haastattelun nauhoitus tallentui sanelukoneen sisäiseen muistiin, eikä sitä siirretty erikseen toiselle työasemalle käsittelyä varten. Haastateltavalle kerrottiin ennen teemahaastattelun aloittamista sen äänittämisestä, josta haastateltavalla oli oikeus kieltäytyä. Yksikään haastateltava ei kieltäytynyt äänittämisestä. Mikäli haastateltava olisi kieltäytynyt haastattelun äänittämisestä, tutkija olisi parhaalla mahdollisella kyvyllään tehnyt muistiinpanoja saamiensa vastausten perusteella. Haastattelun sujuvuus ja vastausten oikeellisuus olisivat kärsineet merkittävästi.

Äänitys helpotti keskeisesti teemahaastattelun toteutusta, sujuvaa etenemistä ja jälkikäteen tapahtuvaa litterointia. Digitaalisen sanelukoneen käyttö helpotti tutkijan keskittymistä haastattelutilanteeseen, kun tarvetta kattavien muistiinpanojen kirjoittamiseen ei ollut. Haastattelu-

jen jälkeen nauhoite kuunneltiin tutkijan toimesta ja kirjoitettiin puhtaaksi jokaisen haastateltavan kohdalla. Haastattelunauhoitteet sekä niiden litteroinnit ovat tutkijan hallussa.

Teemahaastattelut etenivät Pro Gradun lyhyellä esittelyllä, jossa kerrottiin aihe ja päätutkimuskysymys. Tämän jälkeen kerrottiin yleiset ohjeet teemahaastattelun toteutuksesta. Teemahaastattelussa esitettiin kahdeksan alla olevaa kysymystä, joiden jälkeen haastateltaville annettiin mahdollisuus täydentää vastauksiaan ennen haastattelun päättämistä.

1. *Kuinka yleistä BYOD-laitteiden käyttö on tänä päivänä?*
2. *Minkälaiset laitteet ovat yleisimmin käytössä? (päätelaitteen tyyppi / käyttöjärjestelmä)*
3. *Minkälaiseen käyttöön BYOD-laitteet soveltuvat parhaiten?*
4. *Mitä toimenpiteitä BYOD-toimintatapa vaatii organisaatiolta?*
5. *Millaista ohjeistusta tarvitaan?*
6. *Miten BYOD-toimintatavan mahdollisiin tietoturvaongelmiin on valmistauduttu?*
7. *Onko BYOD-toimintatapa lisännyt tietoturvaongelmia?*
8. *Onko BYOD-laitteissa itsessään merkittäviä tietoturvaeroja?*

Teemahaastattelun kysymyksillä saatavien vastausten avulla pyritään ymmärtämään BYOD-toimintatavan laajuus, sisältäen yleisimmät käyttökohteet ja organisaation toimenpiteet. Seuraavassa teemahaastattelun vastaukset käsitellään kysymyskohtaisesti. Vastauksia analysoidaan niiden referoinnin päätteeksi.

5.2. Vastaukset ja niiden analysointi

1. *Kuinka yleistä BYOD-laitteiden käyttö on tänä päivänä?*

Neljä haastateltavaa koki BYOD-laitteiden käytön olevan yleistä ja osana jokapäiväistä työntekoa ja toimintaa, erityisesti pienissä yrityksissä sekä start up-projekteissa. Omia päätelaitteita käytetään työntekoon niin suoraan, kuin myös välillisesti. BYOD nopean yleistymisen seurauksena organisaatioiden oli kehitettävä pakon edessä omat palvelunsa yhteensopiviksi omien laitteiden käytön kanssa. Mikäli organisaatio ei luo toimivaa BYOD-ympäristöä saattavat sen työntekijät käyttää omia laiteita vääriin tarkoituksiin. Tyypillisesti omia päätelaitteita käytetään niissä tilanteissa, kun organisaation antamat laitteet eivät mahdollista työtehtävien tehokasta suorittamista. Yksi haastateltava lähestyi BYOD-käyttöä oman työtehtävänsä kautta, ja totesi oman koneen käytön olevan mahdollista kaksi kolmesta yrityksestä, joissa hän tekee keikkaluonteista työtä. Jäljelle jäävässä kolmanneksessa organisaatio toimittaa hänelle

työaseman, jolla tarvittavat työtehtävät tulisi hoitaa. Organisaation toimialan koettiin vaikuttavan keskeisesti siihen, onko BYOD sallittavissa, mutta samalla nähtiin harvan työtehtävän olevan sellainen, etteikö oman päätelaitteen käyttö olisi millään tasolla mahdollista. Yksi haastateltava arvioi, että BYOD on yleistymässä, vaikkei olekaan varsinaisesti keskustelun aihe yritysten parissa. Organisaatioissa keskitytään käytettäviin palveluihin ja sovelluksiin, jotka ovat käytettävissä niin organisaation laitteilla kuin omilla päätelaitteilla.

Neljä haastateltavaa koki BYOD käytön olevan vähäistä, suurista organisaatioita arviolta vain kymmenen prosenttia sallii BYOD-käytön. Yhtenä syynä vähäiseen käyttöön nähtiin organisaation itse tarjoamat päätelaitteet ja laitteet, joilla päivittäiset työtehtävät turvaluokiteltuine materiaaleineen ovat käytettävissä. Esimerkiksi puolustusvoimilla ei ole tällä hetkellä virallista ohjeistusta omien laitteiden käyttöön, koska työntekijöille jaetaan virkapuhelimet ja tarvittavat päätelaitteet. Yliopistoympäristössä BYOD-verkkoon liittyneitä laitteita oli runsaasti, mutta vain kymmenen prosenttia arvioitiin olevan BYOD-laitteita. Yksi haastateltavan mukaan BYOD ei suurissa organisaatioissa saavuttanut odotettua suosiota ja on tänä päivänä vähenemässä. Yksi haastateltava piti realistisena, että BYOD-palvelut otetaan organisaatioissa laajempaan käyttöön, vaikka onkin vielä vähäistä.

BYOD-laitteiden tai ylipäätään BYOD-käyttöä ei koettu samalla tavalla. Osa haastateltavista näki ilmiön olevan yleinen, kun taas osa sen olevan jo ohimennyt tapa tehdä työtä. Onko se haastateltavan mielestä BYOD-työskentelyä, mikäli merkitset omaan matkapuhelimeesi kalenteriin tulevan tapaamisen tai soitat yksittäisen työtehtäviin liittyvän puhelun omalla älypuhelimella. Organisaation toimiala vaikuttaa keskeisesti siihen, salliiko se BYOD-käytön. Mitä enemmän työtehtäviin kuuluu turvaluokitellun tiedon käsittely, rajoittaa se omien päätelaitteiden käyttöä. Tämän kaltaisissa tapauksissa työntekijä käyttää organisaation tarjoamaa päätelaitetta, jonka käytöllä pyritään muun muassa minimoimaan riskejä. Saaduissa vastauksissa näkyy haastateltavien työtehtävät, toimintaympäristö sekä omat kokemukset.

2. *Minkälaiset laitteet ovat yleisimmin käytössä?*

Kahdeksan haastateltavan mukaan yleisin käytettävä BYOD-laite on älypuhelin. Vain yksi Haastateltava jätti älypuhelimet mainitsematta. Näkemykset käyttöjärjestelmistä vaihtelivat jonkin verran. Älypuhelinten yleisimmäksi käyttöjärjestelmäksi koettiin Android ja seuraavaksi yleisimmäksi iOS. Älypuhelinten jälkeen seuraavaksi yleisimmässä käytössä pidettiin kannettavia tietokoneita, joiden käyttöjärjestelmänä on version 7 ja 10 Windows tai Applen Mac OS. Linux-kannettavien käyttö on BYOD-käytössä vähäistä ja painottuu tietoturva-alan

työntekijöiden käyttöön. Tablettien käytön koettiin olevan laskussa, eikä osaksi tästä syystä ole yleisesti BYOD-käytössä.

Haastateltavat kokevat älypuhelimen olevan yleisin BYOD-laite. Tarkasteltaessa vallitsevia markkinaosuuksia on Android iOSia suuremmassa käytössä. Tähän vaikuttaa erityisesti se, että Android-käyttöjärjestelmän älypuhelimia on markkinoilla usean laitevalmistajan tuottamina. Älypuhelimen yleisyys BYOD-laitteena on hyvä esimerkki siitä, ettei työntekijöillä ole halua kantaa useampaa samantyylistä laitetta mukanaan. Verrattaessa älypuhelinta tablettiin, on se kokonsa puolesta liikuteltavissa helpommin sekä ominaisuuksiensa osalta samanlainen tai jopa kehittyneempi kuin tabletti. Älypuhelimet ovat näyttöjensä osalta lähes samankokoisia, kuin pienet tabletit. Kasvanut näytön koko mahdollistaa älypuhelimelta lisää käyttömahdollisuuksia ja se lienee osasyy tabletin hiipuvaan suosioon.

3. *Minkälaiseen käyttöön BYOD-laitteet soveltuvat parhaiten?*

Viiden haastateltavan mukaan BYOD-laite soveltuu parhaiten julkisen tiedon käsittelyyn tai ympäristöön, jossa ei ole tiukkaa kontrollia eikä päätelaitteelle ole asetettu suuria rajoituksia. Tällainen voi olla organisaatio, jonka toiminta on yleisestikin hyvin julkista. Mutta esimerkiksi yritysmaailmassa vain marginaalinen osa organisaatioista täyttää tällaisen kriteerin. Mikäli käsitellään arkaluontoisempaa tietoa, päätelaitteen suojaus ja kontrollointi korostuu. Toisin sanoen, mitä enemmän organisaatiossa kontrolloidaan tietoturvapolitiikan kautta sitä, mitä omilla laitteilla voidaan tehdä, niiden käyttöaste laskee ja muuttuu lopulta mahdottomaksi. Tiukasta kontrollista voi myös seurata ohjeistuksen vastaista toimintaa, mikäli se haittaa merkittävästi työntekoa. Vapaassa käyttöympäristössä BYOD-laitteen käyttö muodostuu helpommaksi, koska käyttäjä voi itse hallinnoida laitettaan.

BYOD-laitetta on järkevin käyttää siihen tarkoitukseen, mihin ne on luotu käytettäviksi. Tätä mieltä oli kuusi haastateltavaa. BYOD-laitteen ollessa älypuhelin tai tabletti, soveltuu se parhaiten jokapäiväisten työtehtävien vaatimaan kommunikointiin, kuten puheluihin, verkostoitumiseen, sähköpostiin, kalenteritoimintoihin, pikaviesti- ja sosiaalisen median palveluihin sekä VTC-videoneuvotteluihin. Mobiililaitteilla hyödynnetään tavallisia kuluttajapalveluita, joita omilla laitteilla käytetään muutenkin. Näitä palveluita käytettäessä päätelaitteen tiedot tallentuvat pilvipalveluun tai palvelimeen, jolloin käytettävään päätelaitteeseen ei tarvitse luottaa samassa määrin kuin tavallisesti. Älypuhelin soveltuu pääsääntöisesti tiedon selaamiseen tuottamisen sijaan. Lisäksi älypuhelimen sensoreita, kuten kameraa ja GPS-paikannusta voidaan hyödyntää työtehtävissä. Valokuvat ja videot tallentuvat käyttäjän pilvipalveluun,

jolloin niiden käyttö on mahdollista myös toisilla päätelaitteilla. BYOD-laitteen ollessa kannettava tietokone, soveltuu se käsittelyominaisuuksiensa osalta paremmin tiedon käsittelyyn ja tuottamiseen ollen tämän tyylisissä tehtävissä soveltuvin.
Yksi haastateltava koki BYOD-laitteen soveltuvan yliopistoympäristössä hyvin tiedon hakemiseen, kuten kirjaston aineistojen ja tietokantojen käsittelyyn. Kaksi haastateltavaa kertoi BYOD-laitteen soveltuvan sotilasympäristössä siviilitahojen yhteistoimintaan sekä niin sanotun tässä ja nyt-tiedon käsittelyyn ja viestittämiseen. Tiedon vuotaminen ei sinällään vaaranna joukon toimintaa, koska tieto voidaan salata esimerkiksi paikan- tai puheenpeittämismenetelmällä. Kun vastapuoli saa viestin sisällön purettua, on tieto jo vanhentunutta.

Kolme haastateltavaa korosti BYOD-toimintatavan vapautta eli työntekijälle suodaan mahdollisuus käyttää työtehtävissään päätelaitetta, joka hänelle on tuttu ennestään. Organisaation palveluiden ei pitäisi rajoittua päätelaitteisiin, vaan käytössä olevat sovellukset tulisi olla käytettävissä kaikilla alustoilla. Tekniset toteutukset on rakennettava tukemaan kokonaisuutta ja käytettäviä ratkaisuja.

BYOD-laite soveltuu ominaisuuksiensa osalta parhaiten siihen käyttöön, mihin se on suunniteltukin. Yhtenä koko BYOD-trendin keskeisimpinä ajatuksina on vapaus valita käytettävä päätelaite. Älypuhelin ja tabletti soveltuvat tiedon selaamiseen sekä kommunikointiin eri palveluita käyttäen, kannettava tietokone tiedon käsittelyn lisäksi myös sisällön tuottamiseen. Organisaation sisällä BYOD-käyttöä ohjaa toimiala, tietoturvapolitiikka ja – ohjeistus. Edellä mainitut saattavat estää BYOD-laitteiden käytön kokonaan, mutta tietoturvan näkökulmasta BYOD-laitetta on mahdollista käyttää julkisen tiedon käsittelyssä.

4. *Mitä toimenpiteitä BYOD-toimintatapa vaatii organisaatiolta?*

Neljän haastateltavan mukaan BYOD-käyttö perustuu organisaation tietoturvapoliitikassa tarkoin määriteltyyn BYOD-käyttöympäristöön, joka sisältää muun muassa BYOD-laitteen toiminnallisuudet, sallittavat työtehtävät ja tiedot sekä muut palvelut. Ilman tarkkaa määrittelyä BYODin toimivuutta ei kyetä takaamaan organisaatiossa. Mitä enemmän palveluita annetaan käyttäjälle, sitä laajemmaksi hyökkäyspinta-ala kasvaa ja verkolla on suurempi riski haavoittua. Useiden palveluiden BYOD-käyttö on organisaatiolle suuren kynnyksen takana.

Neljä haastateltavaa korosti riskienhallinnan tärkeyttä osana BYODia. Riskit tunnistamalla organisaation ei ole järkevää käyttää työntekijöiden päätelaitteita sellaisiin käyttötarkoituksiin, joissa aiheutettaisiin organisaatiolle turhaa riskiä. Riskien analysoinnin perusteella on

tehtävä päätös, mitä BYOD-laitteella voidaan tehdä ja minkälaisia toimenpiteitä BYOD-laitteelle tulee tehdä organisaation toimesta. Riskianalyysin perusteella organisaatio voi esimerkiksi tehdä päätöksen, että käytetään ympäristöä, jonka kautta tieto on pilvipalvelussa eikä sitä tallennu itse päätelaitteelle. Lisäksi on ymmärrettävä työntekijöiden ammattitaito sekä työtehtävien luonne operaatioturvallisuuden ja tietoturvallisuuden näkökulmasta.

Kuuden haastateltavan mukaan organisaation tulee laatia kattava tietoturvaohjeistus, jotta päätelaitteen käytöstä saadaan suurin mahdollinen hyöty ja turvallinen käyttö varmistetaan. Organisaation on järkevää asettaa tekniset vaatimukset omille päätelaitteille, jotka määritetään ohjeistuksessa. Se voidaan toteuttaa luomalla lista, jossa on organisaation hyväksymät laitteet tai niiden tekniset ominaisuudet. Ohjeistus on koulutettava organisaation henkilöstölle. Tietoturvakoulutuksessa tuodaan esille merkittävimmät BYOD-riskit, jotka kohdistuvat organisaatioon ja koulutetaan, mihin palveluihin omaa päätelaitetta saa käyttää ja mihin ei. Koulutuksella organisaatio varmistuu henkilöstön riittävästä tietoturvatasosta.

Seitsemän haastateltavaa koki tietotekniset ratkaisut keskeisiksi BYOD-käyttöönotossa. Tietoturvan mekanismit on rakennettava siten, että hyväksytään yksittäisen laitteen mahdollinen vihamielisyys. Organisaation verkon arkkitehtuurin ja tietoturvaratkaisujen ollessa kunnossa verkolle ei kohdistu teoriassa uhkaa. On selvitettävä tietotekniset tarpeet, jotta BYOD-laitetta käyttöönottaessa käytännön toimenpiteet, kuten ohjelmiston asentamiset ja vastaavat on määritelty. Toimenpiteenä organisaatio voi teknisesti estää tiettyjen sovellusten käytön ja toimien rajoittamisen tai vaatia päätelaitteen konfigurointia. Esimerkiksi haitallista koodia sisältäville verkkosivuille ei pääse omalla päätelaitteella organisaation verkon kautta. Organisaation tietoturvakontrollien on havaittava päätelaitteen käytön poikkeavuudet, kuten normaalia suurempien aineistojen hakeminen sekä pyrkimykset käsitellä tietoa, johon ei ole käyttöoikeuksia. Poikkeavuuksien havaitsemisen jälkeen on oltava selvillä, kuinka niihin vastataan. Kun organisaatio kustantaa itse päätelaitteet työntekijöilleen, on niiden yksilöinti ja seuranta yksinkertaisempaa kuin BYOD-laitteiden osalta. Omien päätelaitteiden salauksen päällä oloa tai PIN-koodi kyselyä ei välttämättä kyetä varmistamaan. Organisaation on määritettävä kontrollin taso BYOD-laitteiden kanssa. Nykyajan päätelaitteissa on mahdollista luoda erilliset profiilit työlle ja vapaa-ajalle. Organisaation IT-henkilöstöllä on kontrolli vain laitteen työprofiiliin, jolloin vapaa-ajan tieto on vain käyttäjän itse käsiteltävissä eivätkä työtiedostot sekoitu omien tietojen sekaan. Mikäli päätelaitteessa olevaa tietoa halutaan poistaa, on sen toteuttaminen helpompaa työprofiilia hyödyntämällä. Organisaation määrittelemät ja ohjeistamat BYOD-laitteen tekniset vaatimukset täyttämällä päätelaitteen kirjautuminen organisaation verkkoon sallitaan. Tekninen vaatimus voi olla käyttöjärjestelmäversio, virustorjunta tai vastaava. Suuri

haaste organisaatiolla on tapauksissa, joissa tiedon käsittelyä ja tietoliikennettä ei voida valvoa. Tällöin kokonaisuuden hallinta on vaikeaa. Vaihtoehtona hallintaan on MDM eli Mobile Device Management-tyylinen ohjelma. Lisäksi henkilökohtaisilla käyttöoikeuksilla varmistetaan turvallinen tiedon käsittely. Teknisillä rajoituksilla organisaatio ohjaa loppukäyttäjää tietoturvalliseen suuntaan.

BYODin salliva organisaation on valmistauduttava käyttöönoton mahdollistamiseksi monella osa-alueella. Kaikki perustuu organisaation tietoturvapolitiikkaan, riskianalyysiin sekä niihin perustuvaan BYOD-ohjeistukseen. Organisaation verkon osa-tekijöiden on muodostettava tietoturvallinen kokonaisuus ja luotava edellytykset BYOD-käytölle. Tarvittavan ohjeistuksen sisältöä käsitellään tarkemmin seuraavaan kysymyksen vastauksissa.

5. *Millaista ohjeistusta tarvitaan?*

Viisi haastateltava painotti teknistä ohjeistusta, niin organisaatioiden verkkojen kuin BYOD-laitteiden osalta. BYOD-ohjeistus ei merkittävästi poikkea muusta henkilöstölle annettavasta tietoturvaohjeistuksesta. Lähinnä niiltä osin, mitä tietoa saadaan käsitellä omalla päätelaitteella sen ollessa ajantasaisesti päivitetty. Työntekijöiden käytännönohjeistuksen rinnalle tarvitaan teknistä ohjeistusta siitä, mitä asetuksia on muutettava päätelaitteelta BYOD-käyttöä varten. Ohjeistuksen on otettava kantaa muun muassa päätelaitteilla käytettävien salasanojen vaatimustasoon, suojausasetuksiin, päätelaitteen käyttöjärjestelmän ja sovellusten päivittämiseen sekä omien sovellusten asentamiseen. Lisäksi on otettava kantaa, saako laitevalmistajien omia pilvipalveluita ja varmuuskopiointeja käyttää. Mikäli päätelaite on ohjelmoitu synkronoitumaan pilvipalvelun kanssa saattaa organisaation tietoa siirtyä sinne, mikäli kattavaa ohjeistusta ei ole tehty. Erityisesti Android-laitteissa korostuu se riski, että sovelluksia ladataan kolmansilta osapuolilta. Applen päätelaitteilla ei ole sovellusten osalta yhtä suurta riskiä AppStoren tarkemman kontrollin takia. Yhden haastateltavan mukaan omia päätelaitteita käyttäessä muodostuu riski, että käyttäjä siirtää tietoa omalle laitteelle työnteon helpottamiseksi, vaikka se olisi ohjeistuksessa kiellettyä. Organisaatio voi teknisesti estää tämän luomalla dokumentteihin tunnisteen, joka sallii sen käsittelyn vain organisaation verkossa tai sen käyttämässä palvelussa. Tunnisteella estetään dokumentin tai tiedon siirtäminen toisiin sovelluksiin esimerkkinä sosiaaliseen mediaan. Sovelluksen on oltava organisaation hyväksymä, jotta tiedon käyttö sillä olisi mahdollista. Lisäksi kaksi haastateltavaa korosti, että organisaation ohjeistuksen on oltava lyhyt, rautalankatasoinen ja työntekijän helposti lähestyttävissä. Liika ohjeistus koettiin turhaksi.

Kolmen haastateltavan mukaan ohjeistuksen tulee kattaa monia tahoja, ei vain loppukäyttäjiä. Näitä on muun muassa ylläpito-organisaatio sekä organisaation johto. Ohjeistus perustuu elinjaksohallinnan mukaisesti tiettyyn aikajaksoon, milloin BYOD-toimintoja on tarkoitus ylläpitää. Mikäli aikajakson aikana on tarve tehdä laite- tai ohjelmistopäivityksiä on kaikki ohjeistettava etukäteen. Ulkoa ostettu BYOD-palvelu, joka on esimerkiksi 2+2 vuoden sopimuksella eli kaksi vuotta käyttöä ja kahden vuoden jatko-optio, on ohjeistettava koko ajalta, kuinka organisaation eri osat toimivat. Ohjeistuksen tulee kuulua hinnoittelu sekä ongelmatapauksissa tehtävät toimenpiteet, kuten kuka palveluita ylläpitää ja mihin on oltava yhteydessä ongelmatilanteissa. BYOD-laitteen käyttö ei ole yhtään sen helpompi ratkaisu kuin muualta hankittu laite, vain päätelaite vaihtuu.

Organisaation ymmärtäessä BYOD-toimintaympäristön kokonaisuuden, kykenee se määrittämään tekniset ja käytännön toimenpiteet organisaatiossa. Ohjeistus on uhkien ja mahdollisuuksien optimointia, jonka on tuettava työtehtävien onnistunutta toteutusta vaarantamatta organisaation päätehtävien toteutusta. Ohjeistuksen on oltava selkeä, lyhyt ja ajantasainen.

6. Miten BYOD-toimintatavan mahdollisiin tietoturvaongelmiin on valmistauduttu?

Viiden haastateltavan mukaan organisaatiot ovat valmistautuneet BYOD-toimintatavan mahdollisiin tietoturvaongelmiin useilla teknisillä ratkaisuilla. Valmistautumisen taso vaihtelee kuitenkin organisaatioiden välillä paljon. Teknisiä ratkaisuja ovat esimerkiksi palomuurin toteuttaminen, tunkeutumisen havaitsemisjärjestelmien ylläpitäminen, tietoliikenteen seuranta, salaamisratkaisut, virustorjunta, käyttöoikeuksien jakaminen ja lokien hallinta. Organisaation verkot on toteutettu siten, että ne ovat turvallisia. Tekniset ratkaisut pidetään jatkuvasti ajantasaisina. Teknisesti pyritään estämään käyttäjien väärät toimenpiteet mahdollisimman pitkälle rajoittamalla tietynlaiset toiminnallisuudet pois. BYOD-laitteilta vaaditaan pakotetusti riittävän monimutkaisia salasanoja sekä niiden vaihto on suoritettava tasaisin väliajoin. Yksi haastateltavista mainitsee ongelmaksi sen, että laitteet ja käyttöjärjestelmät erityisesti älypuhelimien puolella kehittyvät jatkuvalla tahdilla, jolloin organisaatio on askeleen jäljessä omilla tietoturvaratkaisuillaan, keskitetyllä hallinnallaan ja kontrolleillaan. Toinen haastateltava nostaa mahdolliseksi tavaksi organisaatiolle WEB-applikaation kaltaisen käytön BYOD-ympäristössä. Organisaation käyttäessä WEB-applikaatiota oletuksena on, että päätelaitteet ovat luotettuja ja käytettäessä organisaation päätelaitteiden ohella omia, näin ei välttämättä ole. WEB-applikaatiot on lähtökohtaisesti suunniteltu siten, ettei luoteta käyttäjien päätelaitteisiin.

Yhden haastateltavan mukaan hänen organisaatiossaan BYOD-palveluita ei ole, langatonta BYOD-verkkoa lukuun ottamatta. Palveluiden antamista BYOD-laitteille ei ole koettu tarpeelliseksi, koska organisaation henkilöstölle jaetaan organisaation toimesta päätelaitteet, joilla tarvittaviin tietokantoihin ja palveluihin päästään. Palveluiden minimoimisella on minimoitu myös tietoturvariskit.

Kolme haastateltavan mukaan organisaatiot, joissa ei vielä sallita BYOD-käyttöä ovat valmistautuneet pääasiassa riskianalyysillä ja kartoittamalla potentiaaliset käyttöympäristöt. Samat haastateltavat kokivat aiemmin, ettei BYOD ole yleistynyt heidän organisaatiossaan tai yleisellä tasolla. Näissä organisaatioissa vallitsee hyvä tietoisuus BYODista ja sen mahdollisista riskeistä. Organisaation käyttämien päätelaitteiden tietoturvaongelmia seurataan aktiivisesti, koska käytössä on jo kaupallisia laitteita ja puhelimia, jotka eivät sinänsä eroa BYOD-laitteista. Kahden haastateltavan mukaan voidaan odottaa, että BYOD yleistyy ja puolustusvoimien tulisi kartoittaa käyttötilanteet ja – tavat sekä laatia tarvittava ohjeistus.

Yhden haastateltavan mukaan organisaatiot eivät ole valmistautuneet BYODiin tai jos ovat niin huonosti.

Organisaatioiden valmistautuminen nähtiin rajoittuvan pääasiassa teknisten ratkaisujen toteutukseen. Suurimmaksi osaksi haastateltavat eivät kokeneet BYOD-käytön olevan yleistä, jonka seurauksena toimenpiteistä ei ollut käytännön esimerkkejä.

7. *Onko BYOD-toimintatapa lisännyt tietoturvaongelmia?*

Viisi haastateltavaa yhdeksästä koki, ettei tietoturvaongelmia ole lisääntynyt BYODin myötä. Syiksi mainitaan vähäinen BYOD-käyttö sekä organisaatioiden vahvat suojaukset verkoissa, joihin BYOD-laitteella liitytään. Yksi haastateltava kertoi, ettei ole nykyisessä työtehtävässään kymmenen vuoden aikana kohdannut ainuttakaan merkittävää tietoturvatapahtumaa, joka johtuisi henkilökohtaisen päätelaitteen käytöstä. Syyksi hän mainitsee organisaation valveutuneet käyttäjät, jotka tiedostavat annetun tietoturvaohjeistuksen ja osaavat päätelaitteiden tietoturvallisen käytön. Yksi haastateltava mainitsee, että hyökkäykset kohdistuvat usein käyttäjiin sähköpostin kautta, jolloin varsinainen päätelaite ei ole tietoturvaongelman lisääjä. Neljä haastateltavaa piti tietoturvaongelmien lisääntymistä todennäköisenä, mutta eivät osanneet nimetä tapauksia, milloin näin olisi käynyt. Kaksi haastatelluista piti BYOD-laitteena kannettavan tietokoneen kautta tehtäviä hyökkäyksiä todennäköisempänä kuin älypuhelimen, jonka tietoturvaominaisuuksia he pitivät parempina. Älypuhelimessa tieto on vain sen ohjelman

käytössä, jolla sitä käsitellään. Muut sovellukset eivät pääse siihen käsiksi ellei käyttäjä sitä itse jaa toiselle sovellukselle. Kannettavilla tietokoneilla on kuitenkin se ongelma, että tietoa voi siirtyä muualle, jolloin se lisää tietoturvariskejä.

Tietoturvaongelmien toteutumisesta oltiin eriävää mieltä, mutta haastateltavat nostivat madollisia BYODin tietoturvaongelmia esille. Yhdeksi riskiksi mainittiin MITM eli Man in the middle-tyylinen hyökkäys. Markkinoilla on laitteita, joilla on mahdollista luoda niin sanottu fake-WLAN eli laite kaiutti BYOD-WLANIA, johon käyttäjät liittyvät. Loppukäyttäjälle se näyttää tavalliselta BYOD-WLANilta. MITM-hyökkäyksen käytännön toteuttamista vaikeuttaa se, että laitteen on oltava organisaation toimitiloissa toimiakseen oikein. Käyttäjä liittyy fake-WLAN-verkkoon omilla tunnuksillaan, jolloin BYOD-laitteen liikenne kulkee MITM-laitteen lävitse. Hyökkäyksellä saadaan haltuun tunnukset, salasanat sekä käyttäjän käytössä olevat palvelut. Toisena riskinä ovat huonosti toteutettu verkko tai fyysinen haavoittuvuus organisaation infrassa, mutta kummankaan riskin takana ei ole BYOD-laite. Tietoturvariskinä nähtiin myös se, ettei organisaatiolla ole BYOD-laitteen käyttöön oton yhteydessä varmuutta, mitä laitteella on käsitelty aikaisemmin ja sisältääkö se mahdollisesti vihamielisiä ohjelmia. Yhden haastateltavan mukaan älypuhelimissa lukuisia tietoturvariskejä aiheuttaa käyttöjärjestelmän ulkopuoliset kovakoodatut ominaisuudet. Nämä voivat olla mikrofonin tekemiä tallenteita tai antureiden tietoja, joiden avulla laite toimisi paremmin.

Organisaatiolle BYOD-laitteen hallinnan puute lisää tietoturvaongelmia. Yhden haastateltavan mukaan BYOD-laitteella käsitellessä organisaation tietoja, ei usein tiedosteta sitä, että dokumentit tulisi poistaa päätelaitteelta käsittelyn jälkeen. Organisaation omilta päätelaiteilta tieto voidaan automaattisesti poistaa tietyn ajan kuluttua, mutta omassa laitteessa näin harvemmin on. Tietoturvariski muodostuu, kun BYOD-laite ei ole organisaation hallinnassa ja organisaation dokumentit jäävät laitteelle. Hallinnan puuttuessa päätelaitteista ei välttämättä saada riittävää tietoa eikä organisaatio tiedä, missä sen dokumentteja on tallennettuna.

Vastaukset jakautuivat kahtia, mutta haastateltavat pitivät mahdollisena, että BYOD-laite voi lisätä tietoturvaongelmia. Todennäköisiä tai esimerkkeinä mainittuja riskejä oli useampia, mutta ne eivät ole realisoituneet organisaatioissa.

8. Onko BYOD-laitteissa itsessään merkittäviä tietoturvaeroja?

Kaikki haastateltavat toteavat, että BYOD-laitteissa on tietoturvaeroja, osakseen siksi, että BYOD-laitteiden kirjo on valtava. BYOD-laitteissa on eroja riippuen itse laitteesta ja sen käyttämästä käyttöjärjestelmästä sekä niiden ajantasaisuudesta. Yhden haastateltavan mukaan päätelaitteen, käyttöjärjestelmän tai sovelluksen yleisyys lisäävät todennäköisyyttä niihin kohdistuviin hyökkäyksiin. Se ei kuitenkaan tarkoita suoraan, että yleisin olisi tietoturvaominaisuuksiltaan heikoin, koska päivityksillä vastataan jatkuvasti kohdistuviin uhkiin.

Viisi haastateltavaa korostaa älypuhelimien välisiä tietoturvaeroja, painotuksen ollessa selkeästi Android-päätelaitteissa. Yhden haastateltavan mukaan esimerkiksi Android 7 on hänen mukaansa 18 kertaa turvallisempi kuin Androidin 6 versio. Androidien tietoturva kaatuu sovellusten turvallisuuteen ja käyttöoikeuksiin sekä käyttäjien kuriin. Sovellusta ladatessa käyttäjä antaa paljon oikeuksia kyseiselle sovellukselle ja vaikka niitä muuttaisi jälkikäteen, eivät ne poistu välttämättä Androidin 6 tai vanhemmassa versiossa. Sovelluksen oikeuksilla tarkoitetaan, sitä että esimerkiksi taskulamppu-sovellukselle annetaan oikeudet yhteystietoihin, kameraan, mikrofoniin ja niin edelleen. Mikäli älypuhelin on kaapattu, sen käyttö on komentoperusteista, ei reaaliaikaista. Vihamielisen sovelluksen kautta annetaan komento esimerkiksi mikrofonin aukaisemiseen, äänen tallentamiseen ja nauhoitteen eteenpäin lähettämiseen. Jokainen vaatii siis erillisen komennon. Älypuhelinten tiedonsiirtokapasiteettien rajallisuuden vuoksi niillä voi ottaa ja lähettää kuvia, mutta ei haastateltavan tiedon mukaan lähettämään striimattua videokuvaa. Vihamielisen sovelluksen kautta on mahdollista antaa puhelimelle komento sulkea vain näyttö käyttäjän sammuttaessa puhelimen. Tämän jälkeen voi komennoilla avata kameran ja mikrofonin sekä lähettää nauhoitettua ääntä tai otettuja kuvia eteenpäin. Toisen haastateltavan mukaan nimenomaan Androidin versioiden välillä on suuria eroja. Vanhimmat versiot oli ohjelmoitu, siten että ne ilmoittivat olevansa tietoturvallisia noudattaen kaikkia protokollia ja standardeja, vaikka eivät niitä toteuttaneetkaan. Mobiilikäyttöjärjestelmissä on hallittavuuden osalta merkittäviä eroja. Mikäli käyttöjärjestelmästä tarvitaan tiettyjä tietoja, on sitä kysyttävä suoraan sen valmistajalta ja ylläpitäjältä. Esimerkkinä yksi haastateltava kertoi Ranskan terrori-iskut tehneiden terroristien käyttäneen Windows-puhelimia ja puhelimien paikantamiseksi tarvittiin IMEI-numeroa. Interpol joutui lähestymään Microsoftia, joka antoi tietokannoistaan tarvittavat numerot, jolloin terroristit saatiin paikannettua. Tällainen tietojen luovuttaminen ei ole suuren yrityksen etujen mukaista, koska se antaa käyttäjien laitteista tietoa, jotka se on luvannut pitää vain itsellään. Tämä tarkoittaa, että organisaatiot eivät ole pelkästään tekemisissä tietoturvaongelmien kanssa vaan myös monikansallisten yritysten. Se on aspekti, joka on otettava huomioon, mikäli ongelmia ilmenee ja tietoihin pitää

päästä käsiksi. Se vaikuttaa päätökseen millaiset laitteet organisaatio voi hyväksyä BYOD-käyttöön. BYOD ei ole sen vaarallisempi kuin mikä tahansa elektroniikka mitä organisaatio käyttää, koska vastaavia laitteita käytetään jo. Kyberturvallisuusriskiksi muodostuu, kun organisaatiossa käytetään päätelaitetta, joka ei ole täysin sen hallinnassa hankinnasta alkaen.

Yksi haastateltava kertoo iOS- ja Android-laitteiden välisistä tietoturvaeroista. iOS ekosysteemi on paljon suljetumpi ja kontrolloidumpi ja Apple on sovelluskauppansa osalta Androidin käyttämää Googlen Play Storea tarkempi ladattavista sovelluksista. Androidin yhtenä haasteena ovat laitevalmistajien eroavaisuudet käyttöjärjestelmissä, koska jokainen muokkaus vaikuttaa keskeisesti alkuperäisen Androidin tietoturvaan. Androidin tietoturvasta puhuttaessa on otettava huomioon nimenomaan laitevalmistajien tuomat suuret erot ja tietoturva-arviointi tulisi tehdä jokaisen laitteen kohdalta erikseen. Androidia käyttävät laitevalmistajat useissa tapauksissa lupaavat laitteelle kahden vuoden päivitykset julkaisuhetkestä, jonka jälkeen haavoittuvuuksia ei enää korjata. BYODissa haasteena on se, jos työntekijä on tyytyväinen 2,5 vuotta vanhaan Android-älypuhelimeen, jota laitevalmistaja ei enää päivitä. Apple päivittää iOS-käyttöjärjestelmää myös vanhempiin päätelaitteisiin. Vaikka käyttöjärjestelmä on olevinaan sama, käytössä on kuitenkin toistakymmentä erilaista tuettua versiota. Uudemmat älypuhelimet on kryptattu siten, että salaisen datan käsittely on mahdollista, muutaman vuoden vanhoissa näin ei pääasiassa ole. Mikäli vanhempi älypuhelin saadaan hakkeroitua, on data täysin selväkielistä. Yksi haastateltava ei henkilökohtaisesti suosittelisi organisaatioille minkään muun laitevalmistajan Android-laitetta kuin Googlen omia laitteita, koska toisten valmistajien versioissa on tehty muokkauksia. Muokkaukset yleensä heikentävät alkuperäisen Androidin tietoturvaa.

Haastateltavien vastauksien perusteella älypuhelimissa ja muissa mobiilipäätelaitteissa Android on tietoturvaominaisuuksiltaan iOS-käyttöjärjestelmää heikompi. Pääsyynä ovat sen useat käyttöjärjestelmäversiot, joita eri laitevalmistajat ovat vielä itse muokanneet tuotteelleen sopivammaksi. Androidiin tehtävät muutokset heikentävät sen turvallisuusominaisuuksia merkittävästi. Androidissa haasteeksi koettiin myös päivitystuen loppuminen päätelaitteen ollessa niin sanotusti liian vanha.

6. YHTEENVETO JA JOHTOPÄÄTÖKSET

Bring Your Own Device-toimintatapa sisältää normaalioloissa valtavasti potentiaalia ja sen oikealla valjastamisella organisaation toiminta muuttuu tehokkaammaksi. Henkilökohtaiset päätelaitteet ovat aina työntekijöiden ulottuvilla, niiden käyttö on helppoa ja luonnollista. BYOD-laiteella tarkoitetaan tässä tutkimuksessa älypuhelinta, tablettia tai kannettavaa tietokonetta, jolla tehdään töitä internet-yhteyden välityksellä käsitellen organisaation tietoja. Organisaatiota tarkastellaan geneerisenä käsitteenä rajaamatta tarkemmin tiettyä toimialaa pois käsittelystä. Oletuksena on, että jokaisella organisaatiolla on hallussaan tietoja, joita se ei halua antaa ulkopuolisille tahoille. Tietoa voidaan suojella lain velvoittamana tai sen taloudellisen merkityksen takia. Tutkimuksen pääkysymyksenä on ”*Millainen tietoturvariski BYOD-laite on organisaatiolle?”*. Pääkysymykseen kattavan vastauksen saamiseksi, asetettiin kolme alakysymystä, jotka käsitellään seuraavaksi yksi kerrallaan. Lopuksi vastataan tutkimuksen pääkysymykseen.

Ensimmäinen alakysymyksenä on *”Millaisia tietoturvauhkia kohdistuu organisaatioihin?”*. Kysymykseen saatiin vastaus kirjallisuusanalyysillä. Organisaatioihin kohdistuu tietoturvauhkia monista eri syistä ja eri tahojen toimesta. Organisaation omistama tieto voi olla ulkopuolisen käsissä esimerkiksi taloudellisesti hyödyllinen tai sitä voidaan käyttää vallan välineenä. Viestintäviraston kyberturvakeskuksen Tietoturva vuosi 2017-julkaisussa viideksi suurimmaksi tietoturvauhiksi arvioidaan päätelaitteiden päivitysten laiminlyönti, kiristyshaittaohjelmat, tietoja kalastelevat huijausviestit, ulkoistusten ja laitehankintojen hallinta sekä hyökkäysuhkaukset. Kyberturvakeskus toteaa raportissaan yleisimpien uhkien olleen samansuuntaiset lähivuosina. Viidestä suurimmasta uhasta vain ulkoistusten ja laitehankintojen hallinta ei kosketa BYOD-laitetta. Muut neljä voivat teoriassa tapahtua BYOD-laitetta käyttäessä. Päätelaitteiden päivitysten laiminlyönti luo vihamieliselle taholle hyvät mahdollisuudet hyökkäyksen onnistumiselle. BYOD-laite, joka ei ole ajantasaisesti päivitetty sisältää vakavia haavoittuvuuksia ja on hyvä alusta haittaohjelmien, hyökkäysten ja tietomurtojen nopealle leviämiselle. Päivitysten laiminlyönnin seurauksena esimerkiksi kiristyshaittaohjelmat, kuten toukokuussa 2017 tuhoa tehnyt WannaCry-haittaohjelma voivat levitä organisaation verkkoon. Kiristyshaittaohjelma lukitsee saastuneen päätelaitteen tiedostot, jotka käyttäjä saa haltuunsa vaadittujen lunnaitten maksamisen jälkeen. Organisaatioille merkittävä tietoturvauhka muodostuu myös yksittäisiin henkilöihin tai ryhmiin kohdistettavilla tietojen kalasteluviesteillä. Tietojen kalastelulla pyritään saamaan työntekijöiden kirjautumistunnuksia, joiden avulla ulkopuolinen taho pääsee käsiksi haluamaansa organisaation tietoon. Teemahaastattelussa yksi haastateltavista totesi jopa 90 prosenttia tietomurroista lähtevän loppukäyttäjän huijaamisella.

Tietojen kalasteluun hyödynnetään usein työntekijän käyttämää sähköpostipalvelua. Ulkopuolinen taho esiintyy lähettämässään sähköpostiviestissä esimerkiksi tietohallinnon edustajana ja viestissä pyydetään käyttäjää vaihtamaan salasanansa sähköpostiviestissä oleva linkin kautta. Vaihtaessaan käyttäjätunnuksensa ja salasanansa linkistä avautuvalla sivustolla luovuttaa työntekijä tietämättään kirjautumistunnukset ulkopuoliselle. Näin voi periaatteessa käydä niin omalla kuin organisaation päätelaitteella, eikä ole vain BYOD-laitteen kautta muodostuva uhka. Lähivuosina on yleistynyt tapa, jolla organisaatiota kiristetään uhkaamalla tietomurrolla tai muilla hyökkäyksillä. Uhkaus harvemmin toteutuu, koska sen on tarkoitus aiheuttaa pelkoa organisaation johdossa ja saada heidät maksamaan tietty summa uhkauksen tekijälle. Uhkaus lähetetään tietojen kalastelujen tavoin sähköpostitse.

Toisena alakysymyksenä tutkimuksessa on ”*Miten BYOD-päätelaitteiden käyttöjärjestelmät poikkeavat tietoturvaltaan?”*. Alakysymykseen saatiin vastauksia niin kirjallisuusanalyysin kuin teemahaastattelujen kautta. Kysymyksen taustalla on ajatus siitä, onko jokin BYOD-laitteiden käyttöjärjestelmä turvattomampi ja sitä kautta suurempi tietoturvariski organisaatiolle. Kaikkiin BYOD-laitteiden käyttöjärjestelmiin kohdistuu erilaisia tietoturvahyökkäyksiä eli yksikään ei välty niiltä. Tutkimuksessa havaittiin yhtäläisyys käyttöjärjestelmän yleisyyden ja siinä havaittujen haavoittuvuuksien välillä. Mitä yleisempi käyttöjärjestelmä ja suurempi päätelaitteiden lukumäärä, sitä enemmän vihamieliset tahot pyrkivät hyödyntämään sen heikkouksia omien päämääriensä saavuttamiseksi. Maailman markkinaosuudeltaan yleisimmässä Androidissa on raportoitu olevan eniten haavoittuvuuksia. Yleisimpiin käyttöjärjestelmiin kohdistetaan hyökkäyksiä enemmän kuin toisiin, koska vihamielinen taho hyötyy enemmän – esimerkiksi taloudellisesti - saadessaan haittaohjelmansa mahdollisimman monelle päätelaitteelle. Androidin osalta haavoittuvuuksien raportointiin on myös muita syitä kuin yleisyys.

BYOD-laitteiden kirjo on valtava. Puhuttaessa mobiililaitteista, kuten älypuhelimista ja tableteista useimmin käytettäviä käyttöjärjestelmiä ovat Googlen Android ja Applen iOS. Kirjallisuusanalyysin perusteella Android-käyttöjärjestelmästä nousi esille useita riskitekijöitä. Android ei ole käyttöjärjestelmänä yhtä yksiselitteinen kuin iOS. Androidia on vaikea luokitella pelkästään turvalliseksi tai turvattomaksi, koska se on kokonaisuutena kovin pirstaleinen. Niin sanotun puhtaan eli muokkaamattoman Androidin voidaan sanoa olevan vain Googlen itsensä tuottamissa päätelaitteissa, kuten Nexus-tuoteperheessä sekä puhdasta Androidia käyttävissä älypuhelimissa, esimerkiksi uusissa Nokian älypuhelimissa. Muut laitevalmistajat ovat lähtökohtaisesti muokanneet Androidin-käyttöjärjestelmää omiin päätelaitteisiinsa sopivammaksi, jotta laitteen ominaisuudet saadaan toimimaan parhaiten. Jokainen käyttöjärjestelmään

tehtävä pienikin muutos heikentää sen tietoturvaominaisuuksia ja altistaa laitteen helpommin ulkopuolisille uhille. Androidin toinen ongelma on sen useat eri versiot ja niiden päivitystuki. Tutkimusten mukaan Android-mobiililaitetta tuetaan päivityksillä myyntiintulopäivästä maksimissaan seuraavat kaksi vuotta. Päivitysten loppuessa altistuu kyseinen päätelaite helpommin tietoturvauhille, kun sen haavoittuvuuksia ei enää korjata. Androidin osalta organisaatiot joutuvat selvittämään yksittäisten päätelaitteiden osalta, täyttävätkö ne tietoturvavaatimukset ja soveltuvatko ne BYOD-laitteeksi organisaatiossa. Androidiin verrattaessa iOS on käyttöjärjestelmänä yhtenäisempi. Käyttöjärjestelmänä sitä käytetään Applen valmistamissa iPhone-älypuhelimissa sekä iPad-tableteissa. Päivityspaketit asennetaan kaikkiin yhtiön valmistamiin mobiililaitteisiin, jolloin ne muodostavat tietoturvallisemman kokonaisuuden kuin Android-laitteet. Keskeisenä erona Androidin ja iOSin välillä on niiden lähdekoodi. Android perustuu avoimeen lähdekoodiin iOSin taas suljettuun. Avoimuuden taustalla on ajatus siitä, että kaikki voivat luoda sovelluksia ja kehittää käyttöjärjestelmää tietoturvallisempaan suuntaan, koska sen virheet ovat niin sanotusti näkyvillä. Avoimuus on kuitenkin tietoturvan kannalta enemmän huono kuin hyvä asia. Käyttöjärjestelmien sovelluskauppojen käytännöt vaihtelevat, eikä Apple lähtökohtaisesti salli kolmansien osapuolien sovelluksia Googlen tapaan, vaan haluaa pitää kontrollin itsellään. Edellä mainituista Applen iOSin toimintatapa on tietoturvallisempi. Mobiilikäyttöjärjestelmien osalta iOS on kokonaisuutena tietoturvallisempi vaihtoehto, Androidin osalta vain uusimman, puhtaan ja päivitetyn version käyttö BYOD-laitteessa on turvallista.

Kannettavien tietokoneiden yleisimpiä käyttöjärjestelmiä ovat Windows, Mac OS sekä Linux. Keskeisinä havaintoina vertaillessa edellä mainittuja käyttöjärjestelmäperheitä keskenään ovat päivitykset ja haavoittuvuudet. Windowsilla on Androidin tapaan useita eri versioita maailmanlaajuisessa käytössä, joilla on ajallisesti rajallinen päivitystuki. Tällä hetkellä Windows 7 on eniten käytössä oleva versio, jonka normaali päivitystuki on päättynyt 2015 ja Extended-jakso alkuvuodesta 2020. Mac OS ja Linux päivitystuki on ajallisesti pidempi, Linuxilla Long Term Service-versioille jopa viisi vuotta. Tunnettuja haavoittuvuuksia oli eniten Windowsin käyttöjärjestelmissä ja tarkasteltaessa CIS Benchmark-koventamisohjeita myös eniten asetuksia, jotka on muutettava tietoturvallisemman kokonaisuuden varmistamiseksi. Avoimeen lähdekoodiin perustuva Linux on kokonaisuutena turvallinen, koska sen käyttäjät kehittävät käyttöjärjestelmää jatkuvasti parempaan ja tietoturvallisempaan suuntaan. Markkinaosuudeltaan se on marginaalinen verrattuna Windowsiin ja MacOS:sään, eikä osakseen tästä syystä kiinnosta tietoverkkorikollisia hyökättävänä alustana. Käyttöjärjestelmien haavoittuvuuksia vertaillessa Linux jakelut Debian ja Ubuntu sisälsivät selkeästi vähiten kriittisiä

Tietoturvahaavoittuvuuden kautta kaapatulla kannettavalla tietokoneella hakkeri tai vastaava voi reaaliaikaisesti seurata BYOD-laitteen käyttäjän toimintaa tai käyttää omaa istuntoa. Kaapattua kannettavaa voi komentaa reaaliaikaisesti ja useimmissa tapauksissa kaappaaja pääsee käsiksi kaikkeen materiaaliin, jota kannettavalla käsitellään. Teemahaastattelun perusteella älypuhelimien osalta kaapattua laitetta ohjataan komennoilla eikä reaaliaikaisesti, kuten kannettavia tietokoneita.

Kolmantena alakysymyksenä tutkimuksessa on ”*Minkälaisia tietoturvavaatimuksia on BYOD-laitteen sovelluksilla?”*. Älypuhelimiin asennettavat sovellukset ovat potentiaalinen tapa hyökätä kyseiselle laitteelle. Syitä ovat niille älypuhelimen haltijan toimesta myöntämät käyttöoikeudet sekä sovellusten haavoittuvuudet. Sovellusta asennettaessa määritellään, mitkä käyttöoikeudet sovellukselle suodaan. Vanhemmissa käyttöjärjestelmäversioissa esimerkiksi Androidin kohdalla ei ole mahdollisuutta rajoittaa käyttöoikeuksia, vaan käyttäjä hyväksyy ne sovelluksen asentaessaan. BYOD-ohjeistusta laatiessaan organisaation on tiedostettava niin sanotut vihamieliset sovellukset, joilla on pääsy älypuhelimen tietoihin, jota se ei toimiakseen edes tarvitse, kuten esimerkiksi vihamieliseen tarkoitukseen suunniteltu taskulamppusovellus, jolla oli täydet käyttöoikeudet älypuhelimen yhteystietoihin, paikkatietoihin, mikrofoniin sekä kameraan. Vastaavien sovellusten asentaminen on kiellettävä organisaation BYOD-ohjeistuksessa.

Tutkimuksen pääkysymyksenä on ”*Millainen tietoturvariski BYOD-laite on organisaatiolle?”*. BYOD-laiteella käsitellään organisaation tietoa ja suurin riski on tiedon vuotaminen organisaation ulkopuolelle BYOD-laitteen kautta, eikä niinkään haittaohjelmien siirtyminen organisaation IT-infrastruktuuriin, joka on rakennettu suojelemaan organisaatiota ulkopuolisilta uhilta. Tarkasteltaessa alakysymyksiin saatuja vastauksia kirjallisuusanalyysin ja teemahaastatteluiden perusteella, voidaan todeta yksittäisen henkilön ja organisaation roolin merkitys tietoturvariskin muodostumisessa. Päätelaitteiden markkinaosuuksia tutkiessa on huomattavissa älypuhelimien voimakas yleistyminen. Maailmassa älypuhelimien määrä on jo ohittanut käytössä olevien tietokoneiden määrän ja Suomessa älypuhelinten määrä lähestyy kovaa vauhtia tietokoneita, mennen niiden ohi luultavasti lähivuosina. Haastateltavat totesivat älypuhelimen olevan yleisin BYOD-käytössä ja markkinatilanteen kehittyminen tullee vahvistamaan älypuhelimen asemaa käytetyimpänä BYOD-laitteena. Ominaisuuksiltaan älypuhelimet soveltuvat parhaiten tiedon hakemiseen ja selaamiseen, kannettavan tietokoneen soveltuessa paremmin tiedon muokkaamiseen ja tuottamiseen. Tablettien ja älypuhelinten väliset erot ovat kaventuneet älypuhelinten kosketusnäyttöjen kasvamisen myötä, jolloin tablettien käyttö on itse asiassa jopa vähenemään päin. BYOD-laite on muodostaa tietynlaisissa tilanteissa poten-

tiaalisen uhan organisaatiolle, tähän vaikuttaa kuitenkin moni tekijä. BYOD-laitteen käyttö ei muodosta merkittävää uhkaa organisaatiolle, kun sen käyttö on ohjeistettu henkilöstölle oikein. Ohjeistuksessa kerrotaan, minkälaisen tiedon käsittely omalla päätelaitteella on sallittua ja mitä teknisiä edellytyksiä päätelaitteelta vaaditaan. BYOD-laitteelta on vaadittava tietoturvallisuuden varmistamiseksi muutamaa toimenpidettä, kuten laitteen ajantasaista päivittämistä, virustorjuntaohjelmiston asentamista ja käyttöä sekä tarvittavien salasana- ja PIN-koodien käyttöä. Lisäksi kannettavan tietokoneen osalta palomuuriasetukset on oltava kunnossa. Verkkoyhteyden suojaksi on järkevää käyttää VPN-yhteyttä, jolloin liikennöinti on salattua ja turvallisempaa. Organisaation tietoteknisillä ratkaisuilla voidaan tarkistaa päätelaitteen asetusten tila ja tarvittaessa estää päätelaitteella kirjautuminen organisaation verkkoon. Teemahaastattelussa haastateltavat totesivat, etteivät BYOD-laitteiden muodostamat tietoturvauhat ole kuitenkaan realisoituneet organisaatioissa.

Ongelmaksi muodostuu se, että kyse on yksityishenkilön - vaikka onkin organisaation työntekijä – omistamasta päätelaitteesta. Työhön liittyvien tiedostojen lisäksi BYOD-laitteella on suurella todennäköisyydellä työntekijän henkilökohtaisia tietoja, valokuvia ja mahdollisesti myös arkaluontoista henkilökohtaista materiaalia. Lain silmissä organisaatiolla ei välttämättä ole mahdollisuutta laitteen etähallintaan. Minimoidakseen tiedon siirtymisen väärien tahojen käyttöön BYOD-laitteen kautta, olisi järkevä vaihtoehto verkkoselaimen kautta kirjauduttava salattu palvelu. Vastaavanlainen toteutus on jo verkkopankkipuolella, jonne yksityishenkilö kirjautuu henkilökohtaisilla kirjautumistunnuksilla. Käytännössä verkkopankit toimivat kaikilla internetiin yhdistettävillä vanhemmillakin päätelaitteilla, mikäli käytössä on verkkopankin tukema internet-selaimen versio. Palvelu on rakennettu niin turvalliseksi, ettei käytettävällä päätelaitteella muodosteta sille uhkaa. Tieto pysyy pankilla, eikä tallennu itse päätelaitteelle, näin tietoturvauhat kyetään hallitsemaan paremmin. On kyse kuitenkin rahasta, joten on helppo ymmärtää, etteivät pankit ota turhia riskejä vaan kyseinen toimintatapa on tietoturvallinen ja toimiva. Mikäli rahaliikenne saadaan suojeltua tällaisella menetelmällä, miksei organisaation tiedot BYOD-laitetta käyttäessä.

Teemahaastattelun perusteella yleisin BYOD-laite on älypuhelin. Älypuhelin soveltuu ominaisuuksiensa puolesta tiedon selaamiseen ja yleiseen kommunikointiin. BYOD-laitteena älypuhelimelle soveltuisi varsin hyvin verkkopankkipalvelun tapainen etäistunto, jolla selattavaa tietoa ei tallentuisi päätelaitteelle. Kuten aiemmin tutkimuksessa mainittiin, älypuhelimien osalta korostuu sovellusten tietoturvallisuus. Vihamielinen sovellus voi hyödyntää älypuhelimen mikrofonia tai kameraa, lähettäen tallennetun materiaalin internetin kautta eteenpäin. Kaapattuna BYOD-laitteen kautta vihamielinen taho voi saada organisaation tietoa haltuunsa.

Tieto voi joutua organisaation ulkopuolelle myös tapauksissa, joissa se on tallennettuna BYOD-laitteelle ja kyseinen laite katoaa tai varastetaan. Teknisesti BYOD-laite on mahdollista tyhjentää etäyhteyden avulla, esimerkiksi Mobile Device Management-tyyppisellä ohjelmalla. Tämä on oltava kuitenkin huomioituna organisaation BYOD-politiikassa ja -ohjeistuksessa.

Parhaiten BYOD-laite soveltuu julkisen tiedon käsittelyyn ja sen kanssa työskentelyyn. Laitevalmistajien väliset erot käyttöjärjestelmäpuolella ovat suuret eikä BYOD-laitteilla ole turvallista käsitellä turvaluokitukseltaan julkista salaisempaa tietoa. Haastatteluissa nousi esille ajatus, että BYOD-laite ei varsinaisesti poikkea organisaation omasta laitekannasta, jotka ovat vastaavasti usein niin sanottuja COTS-tuotteita eli kaupan hyllyltä ostettuja. Eroavaisuutena on se, että työpäivän päätyttyä organisaation päätelaitteen voidaan olettaa useimmissa tapauksissa jäävän työpisteelle, BYOD-laitteen siirtyessä työntekijän mukana kotiin, jossa sillä selataan internetiä ja käytetään sosiaalista mediaa. On olemassa riski, että BYOD-laitteeseen tallennettu tieto vuotaa ulkopuolelle tai laitteeseen latautuu jotain vihamielistä, esimerkiksi sovelluksen muodossa, joka voi päätyä organisaation verkkoon laitteen liittyessä siihen seuraavana päivänä. BYOD-laitteiden hallinta on keskeinen haaste organisaatiolle. Mikäli ei ole tiedossa, mitä BYOD-laitteella on käsitelty ennen verkkoon liittymistä, sitä ei voida pitää turvallisena. Ilman keskitettyä hallintaa ei voida varmistua siitä, onko BYOD-laite käyttäjänsä toimesta päivitetty ajantasaiseksi käyttöjärjestelmän ja sovellusten osalta. Se vaikuttaa keskeisesti BYOD-laitteiden välisiin tietoturvaeroihin.

BYOD-laitteen tietoturva on keskeisesti sen käyttäjän käsissä, tämä korostui myös teemahaastattelun vastauksissa. Mikäli organisaation riskianalyysiin perustuvaa ohjeistusta ei noudateta, eikä BYOD-laitteelle ole määritelty vaadittuja asetuksia tai sen käyttö on ollut muuten ohjeistuksen vastaista, muodostaa BYOD-laite suuremman tietoturvauhan organisaatiolle.

6.1. Tutkimuksen luotettavuus ja jatkotutkimusaiheet

Tutkimukseen valitut tutkimusmenetelmät soveltuvat hyvin määriteltyjen tutkimusongelmien selvittämiseen. Kirjallisuusanalyysissa luotiin teoriapohja BYOD-käsitteelle ja BYOD-laitteiden käyttöjärjestelmien haavoittuvuuksille. Teemahaastattelu auttoi käsittämään BYOD-toimintatavan laajuutta, BYOD-laitteita sekä kokonaisuuden tietoturvallisuutta. Haastateltaviksi valikoitui ammattilaisia puolustusvoimista sekä kyberturvayhtiö Nixu Oyj:stä, jolla on asiakkaina useita pohjoismaisia suuryrityksiä. Tämä laajentaa käsitteenä organisaatiota sekä myös BYODista saatiin hyvää yleistietoa yritysmaailman puolelta eikä vastaukset rajoittuneet pelkästään puolustusvoimiin organisaationa. Valitut tutkimusmenetelmät tukivat toisiaan an-

taen hyviä vastauksia asetettuihin tutkimuskysymyksiin. Tutkimusmenetelmiä voidaan pitää valideina.

Päätelaitteiden käyttöjärjestelmiä on tutkittu paljon, jonka vuoksi valmiin tutkimustiedon hyödyntäminen on loogista ja järkevää. Täsmällisempää tietoa olisi saatu, mikäli tutkijalla olisi ollut resursseja luoda testiympäristö rajatuille päätelaitteille ja käyttöjärjestelmille. Nyt käyttöjärjestelmien tietoturvasta saatiin suppeahko yleiskuva, joka olisi vaatinut syvällisempää tarkastelua. Haastatteluissa saadut vastaukset vaihtelivat yksilöiden välillä, ollen jopa täysin vastakkaisia. Tähän voi olla syynä se, miten haastateltava itse kokee BYOD-käsitteen. Ennen nyt esitettyjä kysymyksiä olisi voitu kysyä haastateltavalta, miten hän ymmärtää BYOD-käsitteen.

Suuri osa BYOD-julkaisuista ja artikkeleista käsittelevät toimintatapaa melko pintapuolisesti ja sen mukanaan yritykseen tuomia hyötyjä ja haittoja. BYOD-artikkelien näkökulma on usein juuri yritysmaailmassa. Suurin osa julkaisuista näyttäisi kuitenkin painottavan trendin positiivisia vaikutuksia sekä nopeaa yleistymistä.

Tutkielmassa on käytetty useita internet-lähteistä peräisin olevia sähköisiä artikkeleita, tutkimusraportteja ja muuta sisältöä. Internet-lähteiden käyttö in perusteltua käsiteltäessä viimeisimpien vuosien tietoturvahaavoittuvuuksia, joiden tietoa ei ole saatavilla painetussa muodossa. Tutkimusraportit ovat yliopistojen ja tietoturvayhtiöiden julkaisemia. Yliopistojen julkaisemat tutkimukset perustuvat yliopistojen tutkijoiden tekemiin teknisiin vertailuihin ja kokeisiin, joten niitä voidaan pitää luotettavina. Tietoturvayhtiöiden julkaisut ovat ajankohtaisia ja informatiivisia, mutta usein niiden päämääränä on esitellä olemassa olevien haavoittuvuuksien ja uhkien lisäksi yhtiön tuote, joka suojelee käyttäjää raportissa esitellyiltä uhilta. Tästä syystä niiden käyttöön tutkimuksessa on suhtauduttu tietyllä varauksella.

Kirjallisuusanalyysin ja teemahaastatteluiden perusteella älypuhelimen suosio on suurin BYOD-laitteena ja tilastollisesti lukumäärän voidaan olettaa kasvavan perustuen aiempiin vuosiin. Mielenkiintoisia jatkotutkimusaiheita olisivat BYOD-älypuhelimen soveltuvuus puolustusvoimien käyttöympäristössä normaalioloissa tai vaihtoehtoisesti tietyn joukon käyttöön poikkeusoloissa.

LÄHTEET

[1] Raths, D., Are You Ready for BYOD: Advice from the Trenches on How to Prepare Your Wireless Network for the Bring-Your-Own-Device Movement. Questia. Toukokuu 2012. [Viitattu 3.9.2017] Saatavissa: https://www.questia.com/library/journal/1G1-292008620/are-you-ready-for-byod-advice-from-the-trenches-on.

[2] Cisco. *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper*. Julkaistu 7.2.2017. Päivitetty 28.5.2017.[Viitattu 3.9.2017] Saatavissa: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.

[3] Burt J. *BYOD Trend Pressures Corporate Networks.* eWeek. 5.9.2011. s.30-31. [Viitattu 3.9.2017] Saatavissa: http://www.eweek.com/mobile/byod-trend-pressures-corporate-networks.

[4] Ackerman A., Krupp M. FIVE COMPONENTS TO CONSIDER FOR BYOT/BYOD. IADIS International Conference on Cognition and Exploratory Learning in Digital Age (CELDA 2012).

[5] Accenture. Accenture: Kuluttajateknologian yleistyminen työpaikoilla luo haasteita tietohallinnolle. [Viitattu 2.9.2017] Saatavissa: https://www.accenture.com/fi-en/company-accenture-consumer-technology-penetration-workplace-create.

[6] Talouselämä. Tietotekniikan kuluttajistuminen haastaa työnantajat. [Viitattu 2.9.2017] Saatavissa: http://www.talouselama.fi/tebatti/tietotekniikan-kuluttajistuminen-haastaa-tyonantajat-3356450.

[7] IBM Security. Ten Rules for Bring Your Own Device (BYOD) - Learn how to protect corporate data when users use personal devices for work.pdf Maaliskuu 2016.

[8] Andreasson A., Koivisto J. Tietoturvaa toteuttamassa. 1. painos. Helsinki: Tietosanoma, 2013. 291 s. ISBN 978-951-885-344-6.

[9] Puolustusvoimien Johtamisen Tuen Konsepti 2030 1.0 Julkinen. 2016

[10] Valtiovarainministeriö. VAHTI 8/2008, Valtionhallinnon tietoturvasanasto. Helsinki. 2008. ISBN 978-951-804-889-6.

[11] Hirsjärvi, S., Remes, P. & Sajavaara, P. Tutki ja kirjoita. 13.osin uudistettu painos. Helsinki: Kirjayhtymä, 2007. 448 s. ISBN 978-951-265635-6.

[12] Voltti J. BRING YOUR OWN DEVICE-TRENDIN MAHDOLLISUUDET JA HAASTEET YRITYKSILLE. Tietojärjestelmätieteen Pro Gradu. Turku. 2012. Turun Kauppakorkeakoulu. Johtamisen ja yrittämisen laitos. 76 s.

[13] Lunde F., Mattsson G. Bring Your Own Device – Risker och Möjligheter. Kandidaatintyö. Lund. 2012. Ekonomihögskolan, Lunds Universitet. 70 s.

[14] Eronen S. Mobiilikäyttöjärjestelmien tietoturva. Opinnäytetyö. Espoo. 2015. Laurea AMK. Tietojenkäsittelyn koulutusohjelma. 36 s.

[15] Heljaste J-M., Korkiamäki J., Laukkala H., Mustonen J., Peltonen J., Vesterinen P. Yrityksen turvallisuusopas. 1.painos. Helsinki: Helsingin seudun kauppakamari, 2008. 160 s. ISBN 978-952-99823-6-3.

[16] Andress J., Winterfeld S. Cyber Warfare –Techniques, Tactics and Tools for Security Practitioners – Second Edition. Waltham. Syngress, an imprint of Elsevier. 2014. 306 s. ISBN 978-0-12-416672-1.

[17] Järvinen P., Rousku K. Työpaikan tietoturvaopas: tunnista uhat, hallitse riskit. 1. painos. Helsinki. Alma Talent. 2017. 157 s. ISBN 978-952-14-3049-7.

[18] Hakala M., Vainio M.,Vuorinen O. Tietoturvallisuuden käsikirja. 1. painos. Jyväskylä : Docendo, 2006. 422 s. ISBN 951-846-273-9.

[19] Harris S. CISSP All-in-One Exam Guide – Sixth Edition. 6. painos. New York: McGraw-Hill Education, 2013. 1430 s. ISBN 978-0-07-178174-9.

[20] Valtiovarainministeriö. VAHTI 2/2011, Johdon tietoturvaopas. Helsinki. 2011. ISSN 1798-0860.

[21] Valtiovarainministeriö. VAHTI 5/2013, Päätelaitteiden tietoturvaohje. Helsinki. 2013. ISSN 1798-0860.

[22] Finlex. Ajantasainen lainsäädäntö. [Viitattu: 25.1.2018] Saatavissa: https://www.finlex.fi/fi/

[23] Valtiovarainministeriö. Ohje riskienhallintaan. Helsinki. 2017. Valtiovarainministeriön julkaisuja 22/2017. ISBN: 978-952-251-862-0.

[24] Puolustusministeriö. KATATRI 2015 – Tietoturvallisuuden auditointityökalu viranomaisille. Helsinki. 2015. ISBN: 978-951-25-2682-6.

[25] Valtionvarainministeriö. VAHTI 3/2007 Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Helsinki. 2007. ISBN 978-951-804-768-4.

[26] Valtiovarainministeriö. VAHTI 11/2006 Tietoturvakouluttajan opas. Helsinki. 2006. ISBN 951-804-667-0.

[27] Cisco. *Annual Cybersecurity Report 2018.* pdf.

[28] Haikala I., Järvinen H-M. Käyttöjärjestelmät. 2. painos. Helsinki: Talentum, 2004. 246 s. ISBN 952-14-0851-0.

[29] Silberschatz A., Galvin PB., Gagne G. Operating Systems Concepts Essential – Second Edition. Wiley. 2013. 782s. ISBN 9781118804926.

[30] Viestintävirasto. Tietoturvan vuosi 2017. Helsinki. Viestintäviraston julkaisu. 2018. pdf.

[31] Oppliger R., Internet and Intranet Security - Second edition. Boston. Artech House, 2002. 403 s. ISBN 1-58053-166-0.

[32] Harris J., Ives B., Junglas I. IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. MIS Quarterly Executive. Syyskuu 2012. s. 99-112. ISSN 1540-1979.

[33] Coates S. BYOD Business Issuess. Internal Auditor. Helmikuu 2014. s. 21-23. pdf.

[34] Kendrick J. The ABCs of BYOD for the SMB. ZDNet. [Viitattu 2.9.2017] Saatavissa: http://www.zdnet.com/article/the-abcs-of-byod-for-the-smb/.

[35] Coates S. BYOD Implementation Roadmap. [Viitattu 27.8.2017] Saatavissa: http://www.internalauditor.me/article/byod-implementation-roadmap/.

[36] Koh EB., Oh J., Im C. A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment. Proceedings of the International MultiConference of Engineers and Computer Scientists 2014 Vol II, IMECS 2014, March 12 - 14, 2014, Hong Kong

[37] Esimerkkiorganisaation BYOD-tilasto. Alkuperäinen tiedosto tutkijan hallussa.

[38] Vankka J. Maavoimien taktisen verkon tekniikat ja standardit. Riihimäki: Viestikoulu, 2009. 383 s. ISBN 978-951-25-2025-1.

[39] Statcounter. *Desktop vs Mobile vs Tablet Market Share Finland – January 2018*. [Viitattu: 3.2.2018] Saatavissa: http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/finland

[40] Statcounter. *Desktop vs Mobile vs Tablet Market Share Worldwide – January 2018.* [Viitattu: 3.2.2018] Saatavissa: http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

[41] Zaidi SFA., Shah MA., Kamram M., Javaid Q., Zhang S. *A Survey on Security for Smartphone Device*. International Journal of Advanced Computer Science and Applications, Vol 7. No. 4. 2016.

[42] SANS Institute. *Hardening BYOD: Implementing Critical Security Control 3 in a Bring Your Own Device (BYOD) Architecture.* pdf Syyskuu 2017. 60s.

[43] Bednar J. *Left to Their Own Devices*. BusinessWest. 2016. Kesäkuu 13. s.30-37.

[44] Stallings W. *Wireless Communications & Networks*. 2. painos. Upper Saddle River, NJ : Pearson Prentice Hall, 2005. 559 s. ISBN 0-13-196790-8.

[45] Yesilyurt M., Yalman Y. *Security Threats on Mobile Devices and their Effects: Estimations for the Future.* International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.13-26.

[46] Viestintävirasto. *Haavoittuvuudet.* Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet.html.

[47] Viestintävirasto. *Apple iOS 7.0.2 korjaa kaksi haavoittuvuutta*. [Viitattu 25.1.2018] Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2013/haavoittuvuus-2013-124.html.

[48] Viestintävirasto. *Apple OS X -käyttöjärjestelmän päivitys 2013-004*. [Viitattu: 25.1.2018] Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2013/haavoittuvuus-2013-119.html.

[49] Viestintävirasto. *Androidin lokakuun päivityspaketti julkaistu*. [Viitattu: 25.1.2018] Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2016/haavoittuvuus-2016-126.html

[50] Viestintävirasto. *Nuoret huolehtivat ohjelmistojen päivittämisestä vanhempia paremmin*. [Viitattu 23.1.2018] Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/08/ttn2017082312 01.html

[51] Google. *Android Security 2017 Year in Review.* Maaliskuu 2018. pdf.

[52] Statcounter. *Operating System Market Share Worldwide*. [Viitattu 3.2.2018] Saatavissa: http://gs.statcounter.com/os-market-share

[53] Statcounter. *Operating System Market Share Finland*. [Viitattu 3.2.2018] Saatavissa: http://gs.statcounter.com/os-market-share/all/finland

[54] Microsoft. *Tuotteet, joiden tuki päättyy 2017*. [Viitattu 2.3.2018] Saatavissa: https://support.microsoft.com/fi-fi/help/4001737/products-reaching-end-of-support-for-2017

[55] Microsoft. *Facts About Microsoft.* [Viitattu 17.2.2018] Saatavissa: https://news.microsoft.com/facts-about-microsoft/#About

[56] NetMarketshare. *Operating System Market Share.* [Viitattu 15.1.2018] Saatavissa: https://www.netmarketshare.com/operating-system-market-share.aspx

[57] Microsoft. *Windows-elinkaaren tietosivu*. [Viitattu 2.3.2018] Saatavissa: https://support.microsoft.com/fi-fi/help/13853/windows-lifecycle-fact-sheet

[58] Android. *Security and backround.* [Viitattu 15.1.2018] Saatavissa: https://source.android.com/security/#background

[59] Apple. iOS Security Guide – iOS11. tammikuu 2018. pdf

[60] Apple. *macOS. It's why there's nothing else like a Mac.* [Viitattu 20.12.2017] Saatavissa: https://www.apple.com/macos/what-is/

[61] Kernel.org. *About Linux Kernel.* [Viitattu 6.3.2018] Saatavissa: https://www.kernel.org/linux.html

[62] Kuutti W:, Linux-käsikirja. 1.painos. Jyväskylä: Docento, 2011. 344 s. ISBN 978-951-0-37677-5.

[63] Debian. *Security.* [Viitattu 20.2.2018] Saatavissa: https://www.debian.org/security/

[64] Ubuntu. *Tapaa Ubuntu*. [Viitattu 10.3.2018] Saatavissa: https://www.ubuntu-fi.org/

[65] Debian. *About Debian.* [Viitattu 20.2.2018] Saatavissa: https://www.debian.org/intro/about

[66] NIST. *About NIST*. [Viitattu 10.3.2018] Saatavissa: https://www.nist.gov/

[67] CIS. *About Us.* [Viitattu 10.3.2018] Saatavissa: https://www.cisecurity.org/about-us/

[68] CVE Details. *Current CVSS Score Distribution…* [Viitattu 28.3.2018] Saatavissa: https://www.cvedetails.com/cvss-score-distribution.php

[69] NIST. *Vulnerability Metrics.* [Viitattu 29.3.2018] Saatavissa: https://nvd.nist.gov/vuln-metrics/cvss

[70] CVE Details. *CVSS Score*. [Viitattu 29.3.2018] Saatavissa: https://www.cvedetails.com/cvss-score-charts.php

[71] Norton. *Android vs iOS: Which is More Secure?* [Viitattu 7.2.2018] Saatavissa: https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html

[72] Johnson S., Rashmi VR. *Security in Mobile: A Survey*. International Journal of Computer Applications (0975 – 8887) 2014. s. 24-29.

[73] Thomas DR., Beresford AR., Rice A. *Security Metrics for the Android Ecosystem*.pdf University of Cambridge.

[74] Android. *The Android Story.* [Viitattu 23.1.2018] Saatavissa: https://www.android.com/history/

[75] Android Authority. *Android version distribution: Oreo now installed on 1.1% of Android devices* [Viitattu 18.2.2018] Saatavissa: https://www.androidauthority.com/android-version-distribution-748439/

[76] AVO. *Calculating the score*. [Viitattu 26.3.2018] Saatavissa: http://androidvulnerabilities.org/

[77] Nokia. Puhdas Android. [Viitattu 3.4.2018] Saatavissa: https://www.nokia.com/fi_fi/phones/android

[78] Beaver K. *Android vs. iOS security: Compare the two mobile OSes*. [Viitattu 20.3.2018] Saatavissa: http://searchmobilecomputing.techtarget.com/tip/Android-vs-iOS-security-Compare-the-two-mobile-OSes

[79] CIS. *Microsoft Windows 7 Workstation Benchmark v3.1.0*.pdf Saatavissa: https://www.cisecurity.org/cis-benchmarks/

[80] CIS. *Microsoft_Windows_10_Enterprise_Release_1703_Benchmark_v1.3.0* .pdf Saatavissa: https://www.cisecurity.org/cis-benchmarks/

[81] CIS. *Apple OSX 10.12 Benchmark v1.0.0*.pdf Saatavissa: https://www.cisecurity.org/cis-benchmarks/

[82] CIS. *Apple iOS 11 Benchmark v1.0.0*.pdf Saatavissa: https://www.cisecurity.org/cis-benchmarks/

[83] CIS. *Google Android Benchmark v1.1.0*.pdf Saatavissa: https://www.cisecurity.org/cis-benchmarks/

[84] CIS. *Debian Linux 8 Benchmark v1.0.0*.pdf Saatavissa: https://www.cisecurity.org/cis-benchmarks/

[85] CIS. *Ubuntu Linux 16.04 LTS Benchmark v1.1.0*.pdf Saatavissa: https://www.cisecurity.org/cis-benchmarks/

[86] Wuerthele M.*„Dangerous, targeted iPhone attack nullified by Apple with iOS 9.3.5 patch.* [Viitattu 14.1.2018] Saatavissa: http://appleinsider.com/articles/16/08/25/dangerous-targeted-iphone-attack-nullified-by-apple-with-ios-935-patch

[87] Cambell M., *'Pegasus' iOS malware package also found to impact OS X, Apple issues patch* [Viitattu 14.1.2018] Saatavissa: http://appleinsider.com/articles/16/09/01/pegasus-ios-malware-package-also-found-to-impact-os-x-apple-issues-patch

[88] O'Brien D., *Apple Threat Landscape*.pdf Version 1.02 – February 11, 2016.

[89] Viestintävirasto. *XARA-hyökkäys vaarantaa salasanat ja kirjautumistunnisteet Applen tuotteissa* [Viitattu 10.1.2018] Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/06/ttn2015061811 20.html, 7.3.2018

[90] Nixu Oyj. Esittely. [Viitattu 20.3.2018] Saatavissa: https://www.nixu.com/fi.

TEEMAHAASTATTELUUN OSALLISTUNEET

Haastattelujen materiaali on tutkijan hallussa.

- Aro J-P, Suunnittelija, Maanpuolustuskorkeakoulu. Helsinki. 26.1.2018
- Hämeen-Anttila L, ICT-Järjestelmäpäällikkö, Maanpuolustuskorkeakoulu. Helsinki 7.2.2018
- Jonsson A, Senior Security Specialist, Nixu Oyj. Espoo. 22.2.2018
- Karsikas J, Everstiluutnantti, Sektorinjohtaja, Pääesikunta. Helsinki. 30.1.2018
- Latikka J, Tutkija, Puolustusvoimien tutkimuslaitos. Riihimäki. 16.2.2018
- Nuopponen A, Head of Cyber Defense, Nixu Oyj. Espoo. 22.2.2018
- Penttinen J, Tietohallintopäällikkö, Maanpuolustuskorkeakoulu. Helsinki. 7.2.2018
- Suni N, Senior Software Developer, Nixu Oyj. Espoo. 22.2.2018
- Suomu M, Senior Security Consultant, Nixu Oyj. Espoo. 22.2.2018